TURNING DATA INTO ACTIONABLE IN-TELLIGENCE

ADVANCED FEATURES IN MISP SUPPORTING YOUR ANA-

CIRCL / TEAM MISP PROJECT



MISP PROJECT



Turning data into actionable intelligence

10

2022-09



MISP PROJECT

THE AIM OF THIS PRESENTATION

Turning data into actionable intelligence

└─The aim of this presentation

Why is contextualisation important?
 What options do we have in MISP?
 How can we leverage this in the end?

- Why is **contextualisation** important?
- What options do we have in MISP?
- How can we **leverage** this in the end?

16

THE GROWING NEED TO CONTEXTUALISE DATA

Contextualisation became more and more important as we as a community matured

- **Growth and diversification** 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 a need to be able to prioritise
- These help with filtering your TI based on your requirements...
- ...as highlighted by Pasquale Stirparo Your Requirements Are Not My Requirements

Turning data into actionable intelligence

└─The growing need to contextualise data

THE GROWING NEED TO CONTEXTUALISE DAT

- Contextualisation became more and more important as v as a community matured
- Growth and diversification of our communities
- Distinguish between information of interest and rate
 Extra particle management
- False-positive management
 TTPs and aggregate information may be prevalent com
- to raw data (risk assessment) Increased data volumes leads to a need to be able to
- prioritise
 These help with filtering your TI based on your
- requirements...

 requirements...

 requirements Ai

 requirements Ai

9

60

2022

OBJECTIVES

Turning data into actionable intelligence

└─Objectives

16

6

2022

- Some main objectives we want to achieve when producing
- data Ensure that the information is consumable by everybody
- Ensure that the information is consumable by everybody
 That it is useful to the entire target audience
- The data is contextualised for it to be understood by evenyone
 - What we ideally want from our data
- We want to be able to filter data for different use-cases
 We want to be able to get as much knowledge out of the data for the data of th
 - as possible We want to know where the data is from how it not there
- we want to know where the data is non, now it got there, why we should care

- Some main objectives we want to achieve when producing data
 - Ensure that the information is **consumable** by everybody
 - ► That it is **useful** to the entire target audience
 - The data is contextualised for it to be understood by everyone
- What we ideally want from our data
 - We want to be able to **filter** data for different use-cases
 - We want to be able to get as much knowledge out of the data as possible
 - We want to know where the data is from, how it got there, why we should care

DIFFERENT LAYERS OF CONTEXT

Turning data into actionable intelligence

Different layers of context

Context added by analysts / tools
 Data that tells a story
 Encoding analyst knowledge to automatically leverage the
 above

Context added by analysts / tools

- Data that tells a story
- Encoding analyst knowledge to automatically leverage the above

09-16

Turning data into actionable intelligence —Context added by analysts / tools

-09-16

2022-

CONTEXT ADDED BY ANALYSTS / TOOLS

CONTEXT ADDED BY ANALYSTS / TOOLS

EXPRESSING WHY DATA-POINTS MATTER

Turning data into actionable intelligence

9

-60

2022

Expressing why data-points matter

An IP address by itself is barely ever interesting
 We need to tell the recipient / machine why this is relevant
 All data in MISP has a bare minimum required context

- An IP address by itself is barely ever interesting
 We need to tell the recipient / machine why this is relevant
- All data in MISP has a bare minimum required context
- We differentiate between indicators and supporting data

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

■ 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?

Turning data into actionable intelligence —Context added by analysts / tools

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

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

ى

-60

TAGGING AND TAXONOMIES

Simple labels

- Standardising on vocabularies
- Different organisational/community cultures require different nomenclatures
- Triple tag system taxonomies
- JSON libraries that can easily be defined without our intervention

Tag	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 Context added by analysts / tools

Lagging and taxonomies

 Simple labels 			
Standardising on vocabula	ries		
 Different organisational/co different nomenclatures Triple tag system - taxonoi JSON libraries that can eas intervention 	nies		
194	Evens.	ARCOURT	The
wantowater.competi-			eastlow east-congreet
wantowaste-forst			worklow manufacture
winterstein frompeter	55	10	workfore as a recompeter
waytowater, ordoud,			workflow manufactioner

9

2022-09-

GALAXIES

- 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)

	nware galaxy					
Galaxy ID	373					
Name	Ransomware					
Namespace	misp					
Uuid	3f44af2e-1480-4b6b-9aa8-f9bb213	41078				
Description	Ransomware galaxy based on					
Version	4					
Value 4		Synonyms				
.CryptoHasYou.						
777		Sevleg				
7ev3n		7ev3n-HONE\$T				

Turning data into actionable intelligence —Context added by analysts / tools

-Galaxies

Q

Ś

2022

For the tating, a range strain guess if where
 Some extended sameling results in addition to tatacomic
 Construction to the table of t

Taxonomy tags often non self-explanatory

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 ¹ by Francesco Bigarella from ING
 - **Election guidelines**² by NIS Cooperation Group
- ¹https://www.misp-project.org/galaxy.html#_attck4fraud ²https:

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

Turning data into actionable intelligence —Context added by analysts / tools

> └─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
- 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
- Gave rise to other, ATT&CK-like systems tacking other concerns
 attckufraud 1 by Francesco Bigarella from ING

'https://www.misp-project.org/galaxy.html#_attck&fraud 'https: /https://www.misp-project.org/galaxy.html#_election_guidelines

Q

Ś

DATA THAT TELLS A STORY

Turning data into actionable intelligence

2022-09-16

DATA THAT TELLS A STORY

More complex data-structures for a modern age

Atomic attributes were a great starting point, but lacking in many aspects

- MISP objects³ 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 Data that tells a story

More complex data-structures for a modern age

- Atomic attributes were a great starting point, but lacking i many aspects MISP objects³ system
- Simple templating approact

³https://github.com/MISP/misp-objects

16

-60

SUPPORTING SPECIFIC DATAMODELS

Date	Org	Category	туре		Tags	deleted attributes Galaxies	Comment	Correlate	Related Events
2018-09-28		Name: bank-accou References: 0 🖸							
2018-09-28			status-code: text	A - Active		Add			
2018-09-28			report-code: text	STR Suspicious Transaction Report		Add			
2018-09-28			personal-account-type: text	A - Business		Add			
2018-09-28			swift: bic	HASEHKHH		Add		2	3849 11320 11584
2018-09-28			account: bank-account-nr	788796894883		Add			
2018-09-28			account-name: text	FANY SILU CO. LIMITED		Add			
2018-09-28			currency-code: text	USD		Add			

Turning data into actionable intelligence $\cap{L-}$ Data that tells a story

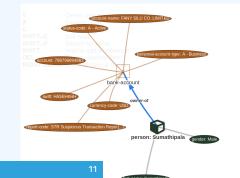
09-16

2022

└─Supporting specific datamodels

|--|

1.0.0		A Mark Parce Nam	the second second	Address of the Address Taxable	·	And and
 -	****	a bite			0	
	-					
		-				
	-					
		-	- 1			
				Contract of 1 (see		



CONTINUOUS FEEDBACK LOOP

Turning data into actionable intelligence

└─Continuous feedback loop

Data shared was frozen in time

- All we had was a creation/modification timestamp
 Improved tooling and willingness allowed us to create
- feedback loop
- Lead to the introduction of the Sighting system
 Signal the fact of an indicator sighting...
- .as well as when and where it was sighted
- Vital component for IoC lifecycle manageme

Data shared was frozen in time

- All we had was a creation/modification timestamp
- Improved tooling and willingness allowed us to create a feedback loop
- Lead to the introduction of the **Sighting system**
- Signal the fact of an indicator sighting...
- ...as well as when and where it was sighted
- Vital component for IoC lifecycle management

ى

-60

2022

CONTINUOUS FEEDBACK LOOP (2)



Turning data into actionable intelligence

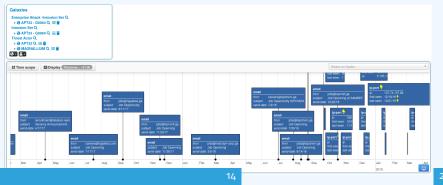
└─Continuous feedback loop (2)

	97.01				
•		CIRCL 2 (2017-03-19 16:17:59)			
۵	NO Income	para	1	1	
•	No interf	00 A 1000		1	
164					
Oute	2015-10	24			
Threat Lev					
Analysis	initial				
Oattributio		et communities			
Sighth	Details Noted				
MIPE	34 Gb - 90	tricked to own organization only.			
	- Dece	_			

09-16

A brief history of time - Adding temporality to our data

- As Andreas said no time based aspect was painful
 Recently introduced **first_seen** and **last_seen** data points
- Along with a complete integration with the **UI**
- Enables the visualisation and adjustment of indicators timeframes



Turning data into actionable intelligence

16

-60

2022-

A brief history of time - Adding temporality to our data

A BRIEF HISTORY OF TIME - ADDING TEMPORALITY TO OUR DATA



THE VARIOUS WAYS OF ENCODING ANALYST KNOWLEDGE TO AUTOMATI-CALLY LEVERAGE OUR TI

Turning data into actionable intelligence —The various ways of encoding analyst knowledge to automatically leverage our TI

2022-09-16

THE VARIOUS WAYS OF ENCODING ANALYST KNOWLEDGE TO AUTOMATI-CALLY LEVERAGE OUR TI

FALSE POSITIVE HANDLING

- Low quality / false positive prone information being shared • Lead to **alert-fatigue**
- Exclude organisation xy out of the community?
- FPs are often obvious can be encoded
- Warninglist system⁴ aims to do that
- Lists of well-known indicators which are often false-positives like RFC1918 networks, ...

LIST OF KNOWN IPV4 PUBLIC DNS RESOLVERS

kl	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		

⁴https://github.com/MISP/misp-warninglists

Turning data into actionable intelligence The various ways of encoding analyst knowledge to automatically leverage our TI

ى

-60-

2022

-False positive handling

Lead to	alert-fatigue	e prone information being sh ut of the community?
	often obvious - ca	
HPS are	often obvious - ca	n be encoded
	elist system' aims	an de abre
		tors which are often
	f well-known indica ositives like RFC19:	
false-p		8 networks,
false-p	ositives like RFC19	8 networks,
false-p	ositives like RFC19	8 networks,
false-p	ositives like RFC19	8 networks,
false-p	ositives like RFC19	8 networks,
false-p	Institutes like RFC19*	8 networks, 9 Warning: Potential faise positive
false-p	ositives like RFC19	Warning: Potential take positive
false-p	Institutes like RFC19*	8 networks, 9 Warning: Potential faise positive

MAKING USE OF ALL THIS CONTEXT

Turning data into actionable intelligence — The various ways of encoding analyst knowledge to automatically leverage our TI

—Making use of all this context

- Providing advanced ways of querying data
- Unified export APIs
 Incorporating all contextualisation options into API filters
- Allowing for an on-demand way of excluding potential false
- positives
 Allowing users to easily build their own export modules feed
 - r various tools

Providing advanced ways of querying data

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

ى

EXAMPLE QUERY

/attributes/restSearch

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

Turning data into actionable intelligence — The various ways of encoding analyst knowledge to automatically leverage our TI — Example query

attributes/resiSearch "returnFormat": "netfilter", "enforce Narninglist": 1, "NOT": ["Type: 05017"] "mip-galay: threat-actors\"Sofary\"", "mip-galay: sectors\"Chemical\""

ى

-60-

EXAMPLE QUERY TO GENERATE ATT&CK HEATMAPS

/events/restSearch

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

Turning data into actionable intelligence

9

,-60-

2022-

—The various ways of encoding analyst knowledge to automatically leverage our TI

Example query to generate ATT&CK heatmaps

/events/restSearch

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

A SAMPLE RESULT FOR THE ABOVE QUERY

A SAMPLE RESULT FOR THE ABOVE QUERY

Turning data into actionable intelligence — The various ways of encoding analyst knowledge to automatically leverage our TI

A sample result for the above query



Pre Attack - Attack Pattern	Enterprise Attack - Atta	ack Pattern Mobile Attack	- Attack Pattern					0		11 🛛 🖉 🕇 Show i
initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Exfiltration	Command and control
Spearphishing Attachment	Scripting	Screensaver	File System Permissions Weakness	Process Hollowing	Securityd Memory	Password Policy Discovery	AppleScript	Data from Information Repositories	Extitration 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
Inusted 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 Extilization	Multi-Stage Channels
Exploit Public-Facing Application	Trusted Developer Utilities	Registry Run Keys / Start Folder	Startup Items	Exploitation for Defense 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	Extilization 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	Extiltration 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	Modity 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

10

,-60-

MONITOR TRENDS OUTSIDE OF MISP (EXAMPLE: DASHBOARD)



Turning data into actionable intelligence ^LThe various ways of encoding analyst knowledge to automatically leverage our TI

> -Monitor trends outside of MISP (example: dashboard)





DECAYING OF INDICATORS

- 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 available context
 - ► Taxonomies
 - Sightings
 - type of each indicator
 - Creation date
 - ► ...

Turning data into actionable intelligence — The various ways of encoding analyst knowledge to automatically leverage our TI

9

2022-09-

-Decaying of indicators

DECAYING OF INDICATORS

- 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 available
- context Taxonomies
- Sightings
- type of ea
 Creation d

21

IMPLEMENTATION IN MISP: Event/view

8+ 2+												
× previous next :	• view all											
+ ≡ ≞ Date † Org	Scope toggi Category	le • 👕 Del Type Value	eted 🔛 Decay score 🕜 Context 🐄 Related Tags		(1) Comment Correlate	Related Feed Events hits	IDSI	Distribution	Sightings	Activity	Enter value to search Score	Q X Actions
2019-09-12	Network activity	ip-src 5.5.5.	5 🐼 + 🚨 +	🕃 + 🚨 +	8		0 1	Inherit	らな / (000)		NIDS Simple Decaying 65.26 Model 5 79.88	••
2019-08-13	Network activity	ip-src 8.8.8.	admirally-scale-source-reliability="a" x retention:expired x	8 + 2 +	×	1222 S1:1 Show S1:2 11 more	8 1	inherit	らな♪ (5/0/0)	uul.	NIDS Simple Decaying 54.6 Model 5 52.69	• • •
2019-08-13	Network activity	ip-src 9.9.9.	9 S admirally-scale:source-reliability="c" x 9 misp:confidence-level="completely-confident" 9 tip:amber x S + +	6+ 1+ ×	×	1 3 19 S1:1 28 Show 6 more	8	inherit	合 <i>ロチ</i> (4/10)		NIDS Simple Decaying 37.43 Model 5 0	• • •

Decay score toggle button

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

Turning data into actionable intelligence — The various ways of encoding analyst knowledge to automatically leverage our TI

9

,-60-

2022-

Implementation in MISP: Event/view



_									
			-						
	• Income		the second						
			100.00			100			
		- 0818	1212		111				-
		Summary of	33		 27				•••
					-		and the second		••
		Server and							-
		- 6819	1210		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 The various ways of encoding analyst knowledge to automatically leverage our TI Implementation in MISP: API result

/artibustion/fetraments/ factopery: Theoret activity", type: "impact", timestamp ": "tablestospor", Lii response in tablestospor", Lii response in tablestospor", descret: sa.a", response in tablestosponse, descret: sa.art, response in tablestosponse, descret: sa.art, response, descret: sa.art, response, descret: sa.art, response, descret: sa.art, response, response,

TO SUM IT ALL UP...

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

Turning data into actionable intelligence — The various ways of encoding analyst knowledge to automatically leverage our TI

└─To sum it all up...

Massive rise in user capabilities
 Growing need for truly actionable threat in
 Lessons learned:

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

ى

2022-09-

GET IN TOUCH IF YOU HAVE ANY QUESTIONS

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

Turning data into actionable intelligence — The various ways of encoding analyst knowledge to automatically leverage our TI

└─Get in touch if you have any questions

Contact us

- https://twitter.com/mokaddem_sa https://twitter.com/iglocska
- Contact CIRCL
- info@circLlu https://twitter.com/c
- https://www.circl.lu/ Contact MISPProject
- Contact MISPProject https://github.com/MISP
- https://gitter.im/MISP/MISP https://twitter.com/MISPProjection

ى

2022-09-