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



THE AIM OF THIS PRESENTATION

Turning data into actionable intelligence

L 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?

-08

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 w is a community matured
- Growth and diversification of our communities
- Distinguish between information of interest and ra Ealse-mosifive 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...

 requirements...

Not My Requirements

∞

6

OBJECTIVES

Turning data into actionable intelligence

└─Objectives

∞

2024-07

- 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 tarret audience
- That it is userul to the entire target audience
 The data is contextualised for it to be understood by provide the second se
- 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 percention
- We want to know where the data is from, how 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

3

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

08

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

2024-07-08

CONTEXT ADDED BY ANALYSTS / TOOLS

CONTEXT ADDED BY ANALYSTS / TOOLS

EXPRESSING WHY DATA-POINTS MATTER

Turning data into actionable intelligence 0-7-0 -Context added by analysts / tools

-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
- We differentiate between indicators and supporting data

ω

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

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

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

ω

2024-07-0

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

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 —Context added by analysts / tools

└─Tagging and taxonomies

Simple labels Standardising on vocabula Different organisational/cc different nomenclatures Triple tag system - taxonou JSON libraries that can eas intervention	ommunity nies		
14	Exem	ANDARS	Tops
wardowates competer			worktow assessments
workfowater-foart			**************************************
wintowate-transport	55	10	worktow as an incompany
workfowater-forgoing*			workburgen (organg)

07-08

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)

🛱 Ranso	mware galaxy	
Galaxy ID	373	
Name	Ransomware	
Namespace	misp	
Uuid	3f44af2e-1480-4b6b-9aa8-f9bb213	341078
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

ω

6

2024

Extractory tags refers non-set-explanatory
 Extractory tags refers non-set-explanatory
 To the tarter, and the tarter of tags of of

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 GALAXIES

- 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
- attcksfraud ¹ by Francesco Bigarella from ING
 Election guidelines ² by NIS Cooperation Group

ω

Turning data into actionable intelligence

DATA THAT TELLS A STORY

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

- MORE COMPLEX DATA-STRUCTURES FOR A MODERN AG
- Atomic attributes were a great starting point, but lacking many aspects
 MISP objects² system
- Simple templating approac
- Use templating to build more complex structure
 Decouple it from the core allow upper to define
 - Decouple it from the core, allow users to define their owr structures
 - MISP should understand the data without knowing the templates
 - Massive caveat: Building blocks have to be MISP attribut types

https://github.com/MISP/misp-object

³https://github.com/MISP/misp-objects

∞

Õ

6

SUPPORTING SPECIFIC DATAMODELS

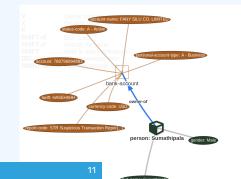
+ Date	Org	Category	Fitters: Type	File Network Financial Proposal Value	Correlation Warnings Include Tags	deleted attributes Galaxies	Show context fields Comment	Q. Corr	claie	Related Events
2018-09-28		Name: bank-accou References: 0 🖸	a2							Í
2018-09-28			status-code: text	A - Active		Add				
2018-09-28			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		•		3849 11320 11584
2018-09-28			account: bank-account-nr	788790894883		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 \Box Data that tells a story

└─Supporting specific datamodels

|--|--|

How Source How Sou	-			-	a holomorphic file on hit.	
		80.10				
		-				
		-				
			-			•



25

07-08

2024

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

-07-08

CONTINUOUS FEEDBACK LOOP (2)



Turning data into actionable intelligence \Box Data that tells a story

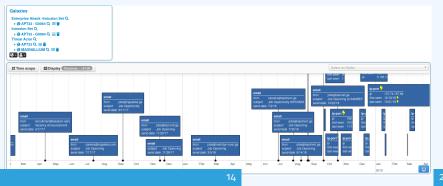
└─Continuous feedback loop (2)

EVE					
•	NO	GROL	a (2017-03-19 16:17:59)		1
8	790	-	page 5	1	1
•	740	inted	002		1
Tapa					
Owne		2015-10-24			
Thread Level		High			
Analysis		initial			
Distribution		Connected on Realized land	mmunitiko		
Sighting C	etala	No. of Concession, Name			
1000		4 (2) - sobick	d to own organization only.		
CROL2		- Dramaion			

2024-07-08

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 $\cap{L-}$ Data that tells a story

ω

01-0

2024-(

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

2024-07-08

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

Id	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)	
/alues		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 Low quality / false positive prone information being shared ω -The various ways of encoding analyst knowledge -01-0 to automatically leverage our TI 2024--False positive handling

	e often obvious - can	be encoded
-	nelist system ⁴ aims t	- de abre
	if well-known indicat	
	positives like RFC1918	
	CONTRACTOR DATE OF THE DESCRIPTION	
*		
a Ser Santas	an La Francisco Marcal Personal Instancio Constante del Constante del Secolo del Marcales	
		Warning: Driverial fairs could
	Industry of the second se	
tan tan	Industry of the second se	Warning: Potential false pos
ter Terlete Terlete Terleter	Industry of the second se	Life of Massies Prof. public DME weathers
ter Terlepe Terlepe Terleperter Terleperter	Industrian and Inf. Washing without a Billing Incom Big Incom	Life of Second Prof. public CAVE second on Top 1000 and solar from News
ter Terlen Se Se	Industrian and Inf. Washing without a Billing Incom Big Incom	Life of Massies Prof. public DME weathers

MAKING USE OF ALL THIS CONTEXT

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
- Incorporating all contextualisation options into API litters
 Allowing for an on-demand way of excluding potential false
- positives Allowing users to easily build their own export modules feed
 - owing users to easily build their own o ir 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

ω

EXAMPLE QUERY

/attributes/restSearch

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

Turning data into actionable intelligence ω ^LThe various ways of encoding analyst knowledge 2024-07 to automatically leverage our TI

-Example query

```
"NOT": [
```

EXAMPLE QUERY TO GENERATE ATT&CK HEATMAPS

/events/restSearch

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

Turning data into actionable intelligence

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

80

2024-07

Example query to generate ATT&CK heatmaps

Example query to generate ATT&CK heatmap

/events/restSearch

"returnFormat": "attack",
"tags": [
 "misp-galaxy:sector=\"Chemical\"
],
"timestamp": "165d"

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



							-		11 Show	
Pre Atlack - Atlack Pattern Initial access	Enterprise Attack - Atta Execution	eck Pattern Mobile Atlaci Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Exfiltration	Command and control
Spearphishing Atlachment	Scripting	Screensaver	File System Permissions Weakness	Process Hollowing	Securityd Memory	Password Policy Discovery	AppleScript	Data from Information Repositories	Extituation 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	Extilization 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	Trusted Developer Utilities	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 Encryp\$on
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	Dynamic Deta Exchange Component Firmware Exdra Window Memory Modity Registry Credentials in Files		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

2024-07-08

MONITOR TRENDS OUTSIDE OF MISP (EXAMPLE: DASHBOARD)



Turning data into actionable intelligence

- L The 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 ω ^LThe various ways of encoding analyst knowledge 2024-07-0 to automatically leverage our TI

-Decaying of indicators

We were still missing a way to use all of these systems in

- Move the decision making from complex filter options complex decay models
- Decay models would take into account various available
- context

IMPLEMENTATION IN MISP: Event/view

« previous	next »	view all													
+ = :	£ >				eed 🗠 Decay score 🛛 Context 💙 Related Tags	T Filtering to								Enter value to search	Q X
Date 1	Org	Category	Туре	Value	Tags	Galaxies	Comment	Correlate	Related Fe Events hit		S Distribution	Sightings	Activity	Score	Actions
2019-09-12		Network activity	ip-src	5.5.5.5	G+ ±+	⊗ + ≗+	1	8			Inherit	16 Q / (01010)		NIDS Simple Decaying 65.26 Model 5 79.88	• • •
2019-08-13		Network activity	ip-src	8.8.8.8	Image: Second state of the s	3 + 2 +	1	×	1222 S1 Show S1 11 more		Inherit	i⇔ © ≯ (5/010)	LLL.	NIDS Simple Decaying 54.6 Model 5 52.69	• • •
2019-08-13		Network activity	ip-src	9.9.9.9 A	admiratly-scale:source-reliability="c" x misp:confidence-level="completely-confident" tip:amber x	3 + ± + ×		×	1 3 19 51 28 Show 6 more	1 2	Inherit	心 心 产 (4/10)	ML.L	NIDS Simple Decaying 37.43 Model 5 0	• • •
2019-08-13		Network activity	ip-src	7.7.7.7	Image: Second state of the se	8 + ± +		8	41	8	Inherit	ich Qr ≱ (3000)	<i>ا</i>	NIDS Simple Decaying 37.41 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 2024-07to automatically leverage our TI

∞

õ

-Implementation in MISP: Event/view



	-	-											
	-			· wearag	-		-						
1000.000										227	sector state		•••
 1000				100	-					27		-	
			-		00					227	And Co.	**	
 Mart et al.			2	100					-		man and a	**	•••
-			33		12/3					27	MARKED AND A		

Decay score toggle button

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

```
/attribute/restarch
*Attribute/restarch
*Turbute/restarch
*Turbute/restarch
*Turbute/restarch
*Turbute/restarch
*Turbute/restarch
*decry.com/file
*search_substarch
*search_substarch_substarch
*search_substarch_substarch_substarch
*search_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_substarch_
```

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 intel
 Lessons learned:
- Context is king Enables better decision making
- Intelligence and situational awareness are natural
- Don't lock users into your workflows, build tools that enable

24

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_ https://twitter.com/iglocska
- https://twitter.com/igld Contact CIRCL
- info@circLlu
- https://twitter.com/circ https://www.circl.lu/
- Contact MISPProject
- https://github.com/MISP https://gitter.im/MISP/MISP
- https://twitter.com/MISPProject

ω