

FROM EVIDENCES TO ACTIONABLE INFORMATION

E.206

CIRCL COMPUTER INCIDENT RESPONSE CENTER LUXEMBOURG

MISP PROJECT

<https://www.misp-project.org/>

MARCH 21, 2022



2022-03-21

From evidences to actionable information

FROM EVIDENCES TO ACTIONABLE INFORMATION

E-206

CIRCL COMPUTER INCIDENT RESPONSE CENTER LUXEMBOURG

MISP PROJECT
<https://www.misp-project.org/>

MARCH 21, 2022



OBJECTIVES OF THIS MODULE

- How evidences can be useful for defense
- Why is contextualisation important
- What options do we have in MISP
- Best practises to encode and contextualise
- How can context be leveraged
- How to structure non-technical information
 - ▶ Practical case: Conti analysis

2022-03-21

From evidences to actionable information

Objectives of this module

OBJECTIVES OF THIS MODULE

- How evidences can be useful for defense
- Why is contextualisation important
- What options do we have in MISP
- Best practises to encode and contextualise
- How can context be leveraged
- How to structure non-technical information
 - ▶ Practical case: Conti analysis

HOW EVIDENCES CAN BE USEFUL FOR DEFENSE

2022-03-21

From evidences to actionable information
└ How evidences can be useful for defense

HOW EVIDENCES CAN BE USEFUL FOR
DEFENSE

The most common recommendations to protect people and assets from cyber attacks are usually:

1. Maintaining softwares up to date
2. Staff awareness
3. Reliable Backups
4. Endpoints protection tools (IDS or SIEM)

From evidences to actionable information
└─ How evidences can be useful for defense

└─ How evidences can be useful for defense

1. An Intrusion Detection System (IDS) is a tool that aims at detecting vulnerability exploits or suspicious activity against a server or a service.
2. A Security Information and Event Management (SIEM) allows centralise security alerts and events generated by endpoints and network devices.

HOW EVIDENCES CAN BE USEFUL FOR DEFENSE

- We can only help endpoints protection tools
- With the proper knowledge and methods, it is possible the maximize their accuracy and performance

These systems can rely on information extracted from

- Log files
- Network captures
- Disk forensic
- ...

However, from a MISP user perspective the hardest part in not to encode the raw evidences, it is to encode them so that they become **actionable**

2022-03-21

From evidences to actionable information
└─ How evidences can be useful for defense

└─ How evidences can be useful for defense

- We can only help endpoints protection tools
- With the proper knowledge and methods, it is possible the maximize their accuracy and performance

These systems can rely on information extracted from

- Log files
- Network captures
- Disk forensic

■ ...
However, from a MISP user perspective the hardest part in not to encode the raw evidences, it is to encode them so that they become **actionable**

WHY IS CONTEXTUALISATION IMPORTANT

2022-03-21

From evidences to actionable information
└ Why is contextualisation important

WHY IS CONTEXTUALISATION IMPORTANT

WHY IS CONTEXTUALISATION IMPORTANT

- Allow the distinction between information of interest and raw data
- provide guidance on how to use this information can be used for for protection
- Filter out noise from information unrelated from the use-case or activity
- Enable risk assessment based on attack type, TTP and threat actor
- Allow triage in large volume of data
- Allow false-positive management

2022-03-21

From evidences to actionable information

└ Why is contextualisation important

└ Why is contextualisation important

1. Tactics, Techniques and Procedures (TTP) describe the context and a detailed description of the behavior taken by an actor

WHY IS CONTEXTUALISATION IMPORTANT

- Allow the distinction between information of interest and raw data
- provide guidance on how to use this information can be used for for protection
- Filter out noise from information unrelated from the use-case or activity
- Enable risk assessment based on attack type, TTP and threat actor
- Allow triage in large volume of data
- Allow false-positive management

Most common expectations of recipients when receiving information

- Being able to **consume** the data
- Find information is **relevant** for them and their partners
- Being able to **understand** the data and its classification
- Assess the **credibility**, likelihood and origin of the data

2022-03-21

From evidences to actionable information

└ Why is contextualisation important

└ Expectations of the recipients

Most common expectations of recipients when receiving information

- Being able to **consume** the data
- Find information is **relevant** for them and their partners
- Being able to **understand** the data and its classification
- Assess the **credibility**, likelihood and origin of the data

Most common expectations of recipients for handling the data

- Being able to **filter** data efficiently for different use-cases
- Obtain as much **knowledge** out of the data as possible
- Know how this data was produced and where its **origin**
- Deduce why is the data **relevant** for them and how **critical** it is

From evidences to actionable information

└ Why is contextualisation important

└ What do recipient hope to do with the data

Most common expectations of recipients for handling the data

- Being able to **filter** data efficiently for different use-cases
- Obtain as much **knowledge** out of the data as possible
- Know how this data was produced and where its **origin**
- Deduce why is the data **relevant** for them and how **critical** it is

IS CONTEXT REALLY THAT IMPORTANT?

- Raw data **is** useful but useless if you don't know what it is about
- That's why it should carry how and why it's relevant

```
1 1.2.3.9
2 137.221.106.104
3 28c643a1f69f9fca9481a4bc9f3f38f3
4 904afe59f6438848be96fd26fdeab01267070d25
5 evil.org
6 accounting.xlsx.exe
7 cat.jpg.exe
```

- In MISP, all data intrinsically have some context
 - ▶ **Type:** ip-src / sha1 / domain
 - ▶ **Category:** network-activity / payload-delivery / external-analysis
 - ▶ **to_ids:** yes / no

2022-03-21

From evidences to actionable information

└ Why is contextualisation important

└ Is context really that important?

1. The 'to_ids' flag is used to differentiate between indicators and supporting data. If the flag is set, it means the attribute is an indicator and is meant for protective tools.

IS CONTEXT REALLY THAT IMPORTANT?

- Raw data is useful but useless if you don't know what it is about
- That's why it should carry how and why it's relevant

```
{
  "id": 1,
  "type": "ip-src",
  "category": "network-activity",
  "to_ids": true,
  "value": "137.221.106.104"
}
```

- In MISP, all data intrinsically have some context
 - ▶ **Type:** ip-src / sha1 / domain
 - ▶ **Category:** network-activity / payload-delivery / external-analysis
 - ▶ **to_ids:** yes / no

IS CONTEXT REALLY THAT IMPORTANT?

- Sometime, more contextual information is not needed as data inherently convey its context:
 - ▶ Tor exit nodes
 - ▶ Botnet / C2 trackers
 - ▶ Ransomwares' bitcoin addresses
 - ▶ ...
- But most of the time, **context is essential**

2022-03-21

From evidences to actionable information

└ Why is contextualisation important

└ Is context really that important?

IS CONTEXT REALLY THAT IMPORTANT?

- Sometime, more contextual information is not needed as data inherently convey its context:
 - ▶ Tor exit nodes
 - ▶ Botnet / C2 trackers
 - ▶ Ransomwares' bitcoin addresses
 - ▶ ...
- But most of the time, **context is essential**

WHAT SORT OF CONTEXT IS PERTINENT

- To what kind of user this data is for
- What type of action can be performed with it
- Estimation on accuracy, reliability and likelihood
- What are the impacts
- For threat actors:
 - ▶ Who is it? What tools were used?
 - ▶ What are their motivations? Who are their targets?
- How can we prevent/detect/block/remediate the attack

From evidences to actionable information

└ Why is contextualisation important

└ What sort of context is pertinent

- To what kind of user this data is for
- What type of action can be performed with it
- Estimation on accuracy, reliability and likelihood
- What are the impacts
- For threat actors:
 - ▶ Who is it? What tools were used?
 - ▶ What are their motivations? Who are their targets?
- How can we prevent/detect/block/remediate the attack

WHAT OPTIONS DO WE HAVE IN MISP

2022-03-21

From evidences to actionable information

└─What options do we have in MISP

WHAT OPTIONS DO WE HAVE IN MISP

MISP offers multiples means to contextualise

- Taxonomies
- Galaxies and Galaxy Clusters
- MITRE ATT&CK
- MISP Objects and relationships
- Sightings and `first_seen` / `last_seen`

Let's have an overview of each of them

From evidences to actionable information

└─What options do we have in MISP

└─What options do we have in MISP

- Simple labels **standardised** on vocabularies
- Taxonomy tags often **self-explanatory**
 - ▶ workflow:state="draft"
 - ▶ doesn't need more explanation
- Triple tag system: namespace:predicate="value"
- Different organisational/community cultures require different nomenclatures
 - ▶ JSON libraries that can easily be defined without the involment of the MISP-project team

<input type="checkbox"/> Tag	Events	Attributes	Tags
<input type="checkbox"/> workflow:state="complete"	11	0	workflow:state="complete" ↗
<input type="checkbox"/> workflow:state="draft"	0	0	workflow:state="draft" ↗
<input type="checkbox"/> workflow:state="incomplete"	55	10	workflow:state="incomplete" ↗
<input type="checkbox"/> workflow:state="ongoing"	0	0	workflow:state="ongoing" ↗

What options do we have in MISP

Taxonomies

2022-03-21

TAXONOMIES

- Simple labels **standardised** on vocabularies
- Taxonomy tags often **self-explanatory**
 - ▶ workflow:state="draft"
 - ▶ doesn't need more explanation
- Triple tag system; namespace:predicate="value"
- Different organisational/community cultures require different nomenclatures
 - ▶ JSON libraries that can easily be defined without the involment of the MISP-project team

Tag	Events	Attributes	Tags
<input type="checkbox"/> workflow:state="complete"	11	0	workflow:state="complete" ↗
<input type="checkbox"/> workflow:state="draft"	0	0	workflow:state="draft" ↗
<input type="checkbox"/> workflow:state="incomplete"	55	10	workflow:state="incomplete" ↗
<input type="checkbox"/> workflow:state="ongoing"	0	0	workflow:state="ongoing" ↗

- Galaxy: Container to group galaxy clusters of the same type
- Galaxy Cluster: knowledge-base item with complex meta-data aimed for human consumption
- Community driven **knowledge-base libraries used as tags**
- Including descriptions, links, synonyms, meta information, etc.
- **Flexible and reusable**
- Works the exact same way as taxonomies but with more **meta-data**
 - ▶ `misp-galaxy:ransomware="CryptoLocker"`
 - ▶ Contains description, reference, documentation and other meta-data

└─What options do we have in MISP

└─Galaxies and Galaxy Clusters

- Galaxy: Container to group galaxy clusters of the same type
- Galaxy Cluster: knowledge-base item with complex meta-data aimed for human consumption
- Community driven **knowledge-base libraries used as tags**
- Including descriptions, links, synonyms, meta information, etc.
- **Flexible and reusable**
- Works the exact same way as taxonomies but with more **meta-data**
 - ▶ `misp-galaxy:ransomware="CryptoLocker"`
 - ▶ Contains description, reference, documentation and other meta-data

Bitcoin Ransomware galaxy

Galaxy ID	373
Name	Ransomware
Namespace	misp
Uuid	3f44af2e-1480-4b6b-9aa8-f9bb21341078
Description	Ransomware galaxy based on...
Version	4

Value ↓

Synonyms

.CryptoHasYou.

777

Sevleg

7ev3n

7ev3n-HONE\$T

2022-03-21

From evidences to actionable information

└─What options do we have in MISP

└─Galaxies and Galaxy Clusters

Galaxies and Galaxy Clusters	
Bitcoin Ransomware galaxy	
Galaxy ID	373
Name	Ransomware
Namespace	misp
Uuid	3f44af2e-1480-4b6b-9aa8-f9bb21341078
Description	Ransomware galaxy based on...
Version	4
Value ↓	Synonyms
.CryptoHasYou.	
777	Sevleg
7ev3n	7ev3n-HONE\$T

- MITRE ATT&CK is one of the best knowledge base of **adversary TTPs**
- **Widely used** and supported by a lot of tools
- The catalogue includes a **matrix-like** interface
- Offers clear visualisation for the kill chain

- MISP Fully support ATT&CK and embraced it's matrix structure
- Multiples matrices for other concerns are available:
 - ▶ Badhra: Similar to ATT&CK but for telecom operators
 - ▶ attck4fraud: Regrouped clusters related to fraud actions

└─What options do we have in MISP

└─MITRE ATT&CK and Galaxy Matrices

1. The kill chain are the sequential steps that adversaries can perform in order to achieve an attack

- MITRE ATT&CK is one of the best knowledge base of adversary TTPs
- **Widely used** and supported by a lot of tools
- The catalogue includes a **matrix-like** interface
- Offers clear visualisation for the kill chain

- MISP Fully support ATT&CK and embraced it's matrix structure
- Multiples matrices for other concerns are available:
 - ▶ Badhra: Similar to ATT&CK but for telecom operators
 - ▶ attck4fraud: Regrouped clusters related to fraud actions

MITRE ATT&CK AND GALAXY MATRICES

2022-03-21

From evidences to actionable information

What options do we have in MISP

MITRE ATT&CK and Galaxy Matrices



Pre-Attack - Attack Pattern	Enterprise Attack - Attack Pattern	Mobile Attack - Attack Pattern								
Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Exfiltration	Command and control
Spearphishing Attachment	Scripting	Screen saver	File System Permissions Weakness	Process Hollowing	Security Memory	Password Policy Discovery	AppleScript	Data from Information Repositories	Exfiltration 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	Exfiltration Over Command and Control Channel	Communication Through Removable Media
Trusted Relationship	User Execution	Trap	Application Shimming	Rootkit	Bash History	Process Discovery	Pass the Hash	Man in the Browser	Data Compressed	Custom Command and Control Protocol
Replication Through Removable Media	Registry/Regasm	System Firmware	Scheduled Task	NTFS File Attributes	Exploitation of Credential Access	Network Share Discovery	Exploitation of Remote Services	Data Staged	Automated Exfiltration	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
Spearphishing Link	Windows Management Instrumentation	LC_LOAD_DLLLIB 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 Doppelganging	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	Timestamp	LLMNR/NBT-NS Poisoning	Network Service Scanning	Remote Services	Audio Capture	Data Transfer Size Limits	Data Obfuscation
Hardware Additions	Dynamic Data Exchange	Component Firmware	Extra Window Memory Injection	Modify 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

Atomic attributes are great, but are lacking a way to express that some can be related to others.

MISP Objects are there to fill the gap:

- **Template system** to build complex structures composed of attributes
- Logically **group attributes** that are contextually linked between each others
 - ▶ A *file* object can contain: a size, name, content, cryptographic hashes, etc.
 - ▶ A *car* object can contain: a brand, a model, a license plate, etc.

From evidences to actionable information

└─What options do we have in MISP

└─MISP Objects

Atomic attributes are great, but are lacking a way to express that some can be related to others.

MISP Objects are there to fill the gap:

- **Template system** to build complex structures composed of attributes
- Logically **group attributes** that are contextually linked between each others
 - ▶ A *file* object can contain: a size, name, content, cryptographic hashes, etc.
 - ▶ A *car* object can contain: a brand, a model, a license plate, etc.

A file object

2018-03-27	Name: file	References: 1
2018-03-27	Payload delivery	filename: putty.exe
2018-03-27	Other	size-in-bytes: 774200
2018-03-27	Other	entropy: 6.7264597226
2018-03-27	Payload delivery	md5: b6c12d88eeb910784d75a5e4df954001
2018-03-27	Payload delivery	sha1: 5ef9515e8fd92a254dd2dcdd9c4b50afa8007b8f
2018-03-27	Payload delivery	sha256: 81de431987304676134138705fc1c21188ad7f27edf6b77a6551aa693194485e
2018-03-27	Payload delivery	sha512: e174ecf4fffb36d30c2cc66b37f82877d421244c924d5c9f39f2e0f37d85332b7d107d5ac5bd19cb7ffdcdbdd8b506d488faa30664ef610f62f3970c163cca76
2018-03-27	Payload delivery	malware-sample: putty.exe

From evidences to actionable information

What options do we have in MISP

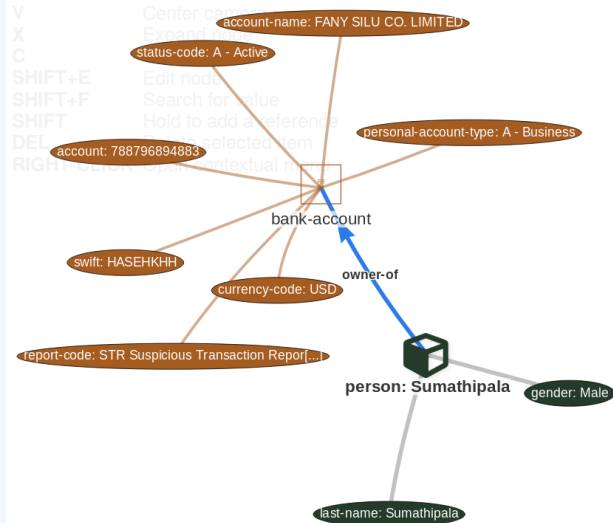
MISP Objects



- Analysts want more than a table of attribute, they want to see how each of them **interact** with the others
- Relationships are essentials to describe scenarios or stories with the data
- MISP allow these relationship to be built between objects

RELATIONSHIPS

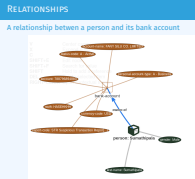
A relationship between a person and its bank account



From evidences to actionable information

└ What options do we have in MISP

└ Relationships



TIMELINESS WITH SIGHTINGS AND `first_seen` / `last_seen`

Adding **Temporality** is a good way to avoid having the data frozen in time

■ Sightings

- ▶ Allows to signal the fact that an indicator was **sighted**
- ▶ They can record the time and where they were the sighting was seen
- ▶ E.g.: Sight C2 servers or phishing websites

■ `first_seen` / `last_seen`

- ▶ These two data-points allow to set when the specified item was first and last seen
- ▶ Enables the visualisation of data timeframe with a timeline
- ▶ *e.g: Track the duration of a campaign or duration for which something was online*

2022-03-21

From evidences to actionable information

└─What options do we have in MISP

└─Timeliness with Sightings and `first_seen` / `last_seen`

Adding **Temporality** is a good way to avoid having the data frozen in time

■ Sightings

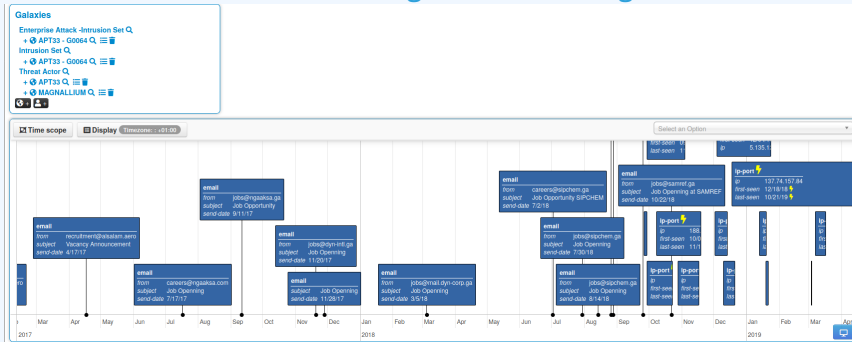
- ▶ Allows to signal the fact that an indicator was **sighted** was seen
- ▶ E.g.: Sight C2 servers or phishing websites

■ `first_seen` / `last_seen`

- ▶ These two data-points allow to set when the specified item was first and last seen
- ▶ Enables the visualisation of data timeframe with a timeline
- ▶ e.g: Track the duration of a campaign or duration for which something was online

TIMELINESS WITH SIGHTINGS AND first_seen / last_seen

Screenshot of the timeline widget when viewing a MISP event



2022-03-21

From evidences to actionable information

└ What options do we have in MISP

└ Timeliness with Sightings and first_seen / last_seen



BEST PRACTISES TO ENCODE AND CONTEXTUALISE

2022-03-21

From evidences to actionable information
└ Best practises to encode and contextualise

BEST PRACTISES TO ENCODE AND CONTEXTUALISE

Always keep in mind that the recipient is a human:

- Include a self-explanatory title
- Make it concise
- Include a report along with the machine parsable data
 - It can either be included as an attribute or as an event-report

It will make the live of the analyst easier: That analyst might end up being you!

From evidences to actionable information
└ Best practises to encode and contextualise
└ Encoding: Event

Always keep in mind that the recipient is a human:

- Include a self-explanatory title
 - Make it concise
 - Include a report along with the machine parsable data
 - It can either be included as an attribute or as an event-report
- It will make the live of the analyst easier: That analyst might end up being you!

Prefer the use of object rather than attributes for attributes intrinsically linked together.

Atomic data by themselves rarely exist: They are often related to something else

- Interactions between elements are frequent
 - ▶ They can often be described by using verbs: connects-to, contain-within, ...
- A story can be inferred without the need to put it into words
 - ▶ *"file was attached to email which when extracted contained a malware connecting to ip-address which was used C2"*
- Properly encoding these relationships turns flat data into a **connected graph**

From evidences to actionable information

- └ Best practises to encode and contextualise
- └ Encoding: Attributes and objects

CONTEXTUALISATION: DISTRIBUTIONS AND PERMISSIBLE ACTIONS

Adding context on **what** actions can be done on the data and **who** can it be shared with

■ Permissible actions taxonomies:

- ▶ *PAP*: Permissible Actions Protocol
- ▶ *IEPF*: Information Exchange Policy (IEP) Framework
- ▶ *pap:white* No restrictions in using this information

■ Sharing level taxonomies:

- ▶ *TLP*: Traffic Light Protocol
- ▶ *IEPF*: Information Exchange Policy (IEP) Framework
- ▶ *tlp:green*: Limited disclosure, restricted to the community

From evidences to actionable information

- └ Best practises to encode and contextualise
- └ Contextualisation: Distributions and permissible actions

- Each data point has a meaning and tells a part of the story
- One should try to capture the answer to these question when contextualising:
 - ▶ In what context was this IoC seen?
 - ▶ Is it related to compromision? Does it tell us anything about the adversary infrastructure?
 - ▶ Was it used to exfiltrate data? Did it acted as a C2?
 - ▶ Did it perform subsequent actions?
 - ▶ ATT&CK can procure even more knowledge

└ Best practises to encode and contextualise

└ Contextualisation: Attributes and their context

- Each data point has a meaning and tells a part of the story
- One should try to capture the answer to these question when contextualising:
 - ▶ In what context was this IoC seen?
 - ▶ Is it related to compromision? Does it tell us anything about the adversary infrastructure?
 - ▶ Was it used to exfiltrate data? Did it acted as a C2?
 - ▶ Did it perform subsequent actions?
 - ▶ ATT&CK can procure even more knowledge

However, think twice before tagging:

- If a tag applies to the whole content of the event, it should be attached on the event instead
- If the tag offers no real utility or hinder your ability to analyse the whole dataset, it should probably be ignored

From evidences to actionable information

└ Best practises to encode and contextualise

└ Contextualisation: Attributes and their context

However, think twice before tagging:

- If a tag applies to the whole content of the event, it should be attached on the event instead
- If the tag offers no real utility or hinder your ability to analyse the whole dataset, it should probably be ignored

CONTEXTUALISATION: ORIGIN, LIKELYHOOD AND RELIABILITY

- The source of information has an impact on how people evaluates its trust
 - ▶ Data without a source / origin might be considered unreliable
 - ▶ *i.e: A research paper without citing its sources is useless*
- MISP bridges people and and communities
 - ▶ The more one is connected, the greater the quantity and diversity of data
 - ▶ Not everything you read on the internet is true!

2022-03-21

From evidences to actionable information

└ Best practises to encode and contextualise

└ Contextualisation: Origin, likelihood and reliability

- The source of information has an impact on how people evaluates its trust
 - ▶ Data without a source / origin might be considered unreliable
 - ▶ *i.e: A research paper without citing its sources is useless*
- MISP bridges people and and communities
 - ▶ The more one is connected, the greater the quantity and diversity of data
 - ▶ Not everything you read on the internet is true!

CONTEXTUALISATION: ORIGIN, LIKELYHOOD AND RELIABILITY

If you can't share the source, provide the trust in the source

- Include the reliability and the credibility of the information
 - ▶ Taxonomy: admiralty-scale
 - ▶ *i.e: admiralty-scale:source-reliability="Usually reliable"*
- Include the quality and likelihood
 - ▶ Taxonomy: estimative-language
 - ▶ *i.e: estimative-language:likelihood-probability="very likely"*

2022-03-21

From evidences to actionable information

└ Best practises to encode and contextualise

└ Contextualisation: Origin, likelihood and reliability

If you can't share the source, provide the trust in the source

- Include the reliability and the credibility of the information
 - ▶ Taxonomy: admiralty-scale
 - ▶ *i.e: admiralty-scale:source-reliability="Usually reliable"*
- Include the quality and likelihood
 - ▶ Taxonomy: estimative-language
 - ▶ *i.e: estimative-language:likelihood-probability="very likely"*

- The purpose is not to blame but to identify the attacker's **intent**
- Knowing the intent greatly help to:
 - ▶ Know the objectives
 - ▶ Understand what are the targeted assets
 - ▶ Deduce the treat level
- It allows to identity behaviors
 - ▶ Might speed up the next investigation
 - ▶ Might bootstrap the analysis procdess

CONTEXTUALISE: PROVIDE ADVICES ON HOW TO PROTECT THEMSELVES

To help recipients to better protect themselves, additional information can be provided.

- Indicate what can be done with the data
 - ▶ Use it to feed an IDS
 - ▶ Perform historical search with a SIEM to find a potential compromise
 - ▶ Inform your peers against a new type of threat
- Provide additional supporting materials
 - ▶ The original report form which the data is coming from
 - ▶ Home-brew scripts
 - ▶ Sigma rules for SIEM searches
 - ▶ Context and configurations under which the analysis was done

2022-03-21

From evidences to actionable information
└ Best practises to encode and contextualise

└ Contextualise: Provide advices on how to protect themselves

To help recipients to better protect themselves, additional information can be provided.

- Indicate what can be done with the data
 - ▶ Use it to feed an IDS
 - ▶ Perform historical search with a SIEM to find a potential compromise
 - ▶ Inform your peers against a new type of threat
- Provide additional supporting materials
 - ▶ The original report form which the data is coming from
 - ▶ Home-brew scripts
 - ▶ Sigma rules for SIEM searches
 - ▶ Context and configurations under which the analysis was done

HOW CAN CONTEXT BE LEVERAGED

2022-03-21

From evidences to actionable information
└─ How can context be leveraged

HOW CAN CONTEXT BE LEVERAGED

Let's make use of this well-structured, context-rich data

- Incorporate all contextualisation options into API filters

```
1 {  
2   "AND": [  
3     "admiralty-scale:source-reliability=\"Reliable\""  
4   ],  
5   "OR": [  
6     "threat-actor=\"Sofacy\"",  
7     "sector=\"Chemical\"",  
8     "country=\"Luxembourg\"",  
9   ]  
10 }
```

From evidences to actionable information

└─ How can context be leveraged

└─ Leveraging the context

Let's make use of this well-structured, context-rich data
■ Incorporate all contextualisation options into API filters

```
{  
  "AND": [  
    "admiralty-scale:source-reliability=\"Reliable\""  
  ],  
  "OR": [  
    "threat-actor=\"Sofacy\"",  
    "sector=\"Chemical\"",  
    "country=\"Luxembourg\"",  
  ]  
}
```

LEVERAGING THE CONTEXT

- On-demande potential false positive exclusion
- Warninglist system helps to exclude known false-positives reducing alert-fatigue

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
Type	string
Accepted attribute types	ip-src, ip-dst, domain ip
Enabled	Yes (disable)

Values

1.0.0.1
1.1.1.1
1.11.71.4

Warning: Potential false positives

List of known IPv4 public DNS resolvers
Top 1000 website from Alexa
List of known google domains

2022-03-21

From evidences to actionable information

- └ How can context be leveraged
- └ Leveraging the context

- On-demande potential false positive exclusion
- Warninglist system helps to exclude known false-positives reducing alert-fatigue

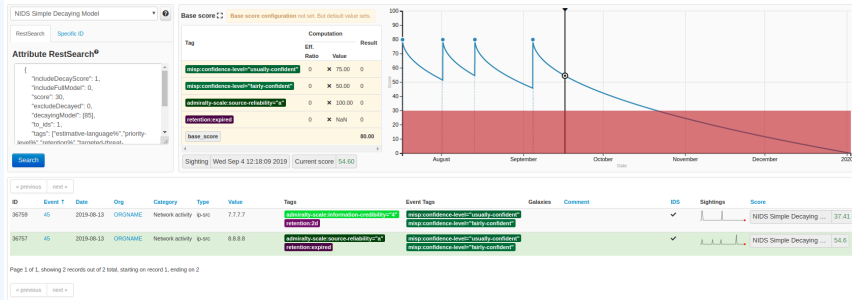
LIST OF KNOWN IPV4 PUBLIC DNS RESOLVERS

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
Type	string
Accepted attribute types	ip-src, ip-dst, domain ip
Enabled	Yes (disable)

Warning: Potential false positives
List of known IPv4 public DNS resolvers
Top 1000 website from Alexa
List of known google domains

LEVERAGING THE CONTEXT

- IoC prioritization and lifecycle management
- Integrate decay models to filter out expired/unrelevant data



2022-03-21

From evidences to actionable information

- └ How can context be leveraged
 - └ Leveraging the context



LEVERAGING THE CONTEXT

■ Allow users to build their own export module

HTTP headers

Authorization: YOUR_API_KEY
Accept: application/json
Content-type: application/json

HTTP body

```
1 {  
2   "returnFormat": "  
3 }
```

Run query

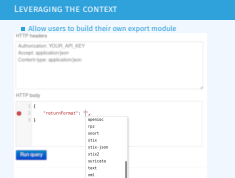
- openioc
- rpz
- snort
- stix
- stix-json
- stix2
- suricata
- text

2022-03-21

From evidences to actionable information

└ How can context be leveraged

└ Leveraging the context



ENABLING COMMON USER PROFILES TO BETTER PERFORM THEIR TASKS

How does different user profiles benefits to most of well-structured, context-rich data

- **incident responder:** Self-explanatory data relieves pressure and reduces the change of misunderstanding it
- **SOC operator:** Reduce alert-fatigue and energy to filter unwanted data
- **ISP:** Ease the task to decide if the data is fit for blocking based on trust and context the data was seen in
- **threat analyst:** Provide insight on the modus operandi and goals of attacker
- **risk analyst:** Help highlighting potential security gaps and formulate advices on preventive actions
- **decision maker:** Guide resources allocation based on current/emerging threats for their region and sector

From evidences to actionable information

└ How can context be leveraged

└ Enabling common user profiles to better perform their tasks

ENABLING COMMON USER PROFILES TO BETTER PERFORM THEIR TASKS

How does different user profiles benefits to most of well-structured, context-rich data

- **incident responder:** Self-explanatory data relieves pressure and reduces the change of misunderstanding it
- **SOC operator:** Reduce alert-fatigue and energy to filter unwanted data
- **ISP:** Ease the task to decide if the data is fit for blocking based on trust and context the data was seen in
- **threat analyst:** Provide insight on the modus operandi and goals of attacker
- **risk analyst:** Help highlighting potential security gaps and formulate advices on preventive actions
- **decision maker:** Guide resources allocation based on current/emerging threats for their region and sector

HOW TO STRUCTURE NON-TECHNICAL INFORMATION

2022-03-21

From evidences to actionable information
└─ How to structure non-technical information

HOW TO STRUCTURE NON-TECHNICAL
INFORMATION

- Identify non-technical data that can be useful for an investigation,
- Illustrate how non-technical and technical data can interact to produce meaningful insights,
- Model these interactions,
- Outline what Socio-Technical interactions are useful to share.

From evidences to actionable information

- └ How to structure non-technical information
 - └ Objectives

1. A note for the slide handout

- Identify non-technical data that can be useful for an investigation,
- Illustrate how non-technical and technical data can interact to produce meaningful insights,
- Model these interactions,
- Outline what Socio-Technical interactions are useful to share.

Computer and their security is linked to human activities:

- Technical traces show human activities,
- Technical traces can convey human intent,
- Human interactions can explain and give context to Technical traces,
- CyberCrime requires infrastructures and logistics that are discussed between humans,
- TTPS are discussed and exchanged,
- Human interaction can help attributing attacks to threat actors,
- Human interaction can help deciphering intent and motives, and discriminate human error from sabotage.

From evidences to actionable information
└─ How to structure non-technical information
└─ We live in Socio-Technical Systems

1. A note for the slide handout

Computer and their security is linked to human activities:

- Technical traces show human activities,
- Technical traces can convey human intent,
- Human interactions can explain and give context to Technical traces,
- CyberCrime requires infrastructures and logistics that are discussed between humans,
- TTPS are discussed and exchanged,
- Human interaction can help attributing attacks to threat actors,
- Human interaction can help deciphering intent and motives, and discriminate human error from sabotage.

Use OSINT and data leaks to:

- bring context to other ransomware cases,
- better understand the gang day to day operations,
- get insights on events' timeline,
- confirm or invalidat previous hypotheses,
- select relevant information to share and produce an intelligence report.

From evidences to actionable information

└─ How to structure non-technical information

└─ Plan

1. A note for the slide handout

Use OSINT and data leaks to:

- bring context to other ransomware cases,
- better understand the gang day to day operations,
- get insights on events' timeline,
- confirm or invalidat previous hypotheses,
- select relevant information to share and produce an intelligence report.

CONTI RANSOMWARE GROUP LEAK ANALYSIS

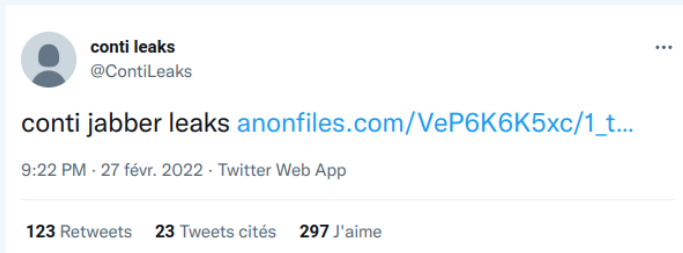
2022-03-21

From evidences to actionable information
└ Conti ransomware group leak analysis

CONTI RANSOMWARE GROUP LEAK
ANALYSIS

RANSOMWARE JABBER CHATS LEAK

Published on Twitter:

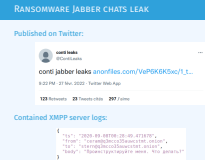


Contained XMPP server logs:

```
{
  "ts": "2020-09-08T00:28:49.471678",
  "from": "ceram@q3mcco35auwcstmt.onion",
  "to": "stern@q3mcco35auwcstmt.onion",
  "body": "Проинструктируйте меня. Что делать?"
}
```

2022-03-21

From evidences to actionable information
└ Conti ransomware group leak analysis
└ Ransomware Jabber chats leak



We use AIL¹ to dig into the data:

- AIL processes the data and search for relevant information
 - ▶ PGP keys,
 - ▶ Bitcoin addresses, maybe others,
 - ▶ onion hidden services,
 - ▶ IP addresses.
- Once we find relevant information we push it into MISP,
- we use MISP correlation engine to find relevant past cases.

¹<https://ail-project.org/>

From evidences to actionable information

└ Conti ransomware group leak analysis

└ Ransomware Jabber chats leak in AIL

1. It is important to understand what we search for before digging into the data with AIL.
2. Gang may discuss payments, so we are interested in crypto currencies
3. Gang may discuss IP addresses and infrastructure, so we are interested in IP addresses, etc.
4. For the training, we use a dedicated AIL container that contains RAW translated jabber chats.

We use AIL¹ to dig into the data:

- AIL processes the data and search for relevant information
 - ▶ PGP keys,
 - ▶ Bitcoin addresses, maybe others,
 - ▶ onion hidden services,
 - ▶ IP addresses.
- Once we find relevant information we push it into MISP,
- we use MISP correlation engine to find relevant past cases.

¹<https://ail-project.org/>

RANSOMWARE JABBER CHATS LEAK IN AIL

Prepare AIL to detect IPv4 addresses by creating a 'tracker':

Create a new Tracker

IP

E-Mails Notification (optional, space separated)

Webhook URL

Tracker Description (optional)

jabber

Tracker Type:

YARA rule

Select a default yara rule or create your own rule:

Default YARA rules:

Select a default rule

Custom YARA rules:

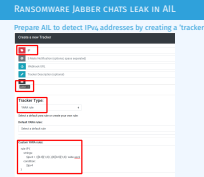
```
rule IP {
  strings:
    $ip4 = /[0-9]{1,3}\.[0-9]{1,3}\.[0-9]{1,3}/ wide ascii
  condition:
    $ip4
}
```

2022-03-21

From evidences to actionable information

Conti ransomware group leak analysis

Ransomware Jabber chats leak in AIL



1. We choose the tag 'IP' to label the relevant items.
2. We select the 'jabber' source, that is to say that this leak hunter rule will only be applied on items coming from the jabber data source
3. We select the tracker type "YARA rule" as we plan to use yara for this leak hunter
4. Finally we write the yara rule containing a regex that matches IPv4 addresses
5. A "regex" leak hunter could do the same job, so why do we prefer using a yara rule tracker instead? Because AIL's retro hunt feature uses yara rules only, therefore it's easier to reuse yara trackers than regex ones.

use MISP to correlate this information from past cases,
■ TODO

2022-03-21

From evidences to actionable information
└ Conti ransomware group leak analysis
└ Dig

1. A note for the slide handout

ease attribution of these past cases through IoC,

- TODO

From evidences to actionable information

- └ Conti ransomware group leak analysis

- └ Dig

1. A note for the slide handout

ease attribution of these past cases through IoC,
■ TODO

add context to past cases from the chats logs in order to ease their investigation,

- TODO

1. A note for the slide handout

support colleagues and other CSIRTs with real Intelligence.

■ TODO

2022-03-21

From evidences to actionable information

└ Conti ransomware group leak analysis

└ Dig

1. A note for the slide handout

- Given the growth and diversification and maturity of users, **contextualisation is becoming essential**
- Well-structured, context-rich data is good as it enables better **decision making**
- It will rise user capabilities and thus **improve protection**
- MISP has a format and tools designed to support contextualised data

Provide sources along with the data!

- Turning data into actionable intelligence - advanced features in MISP supporting your analysts and tools (CIRCL.lu)
 - ▶ <https://www.enisa.europa.eu/events/2019-cti-eu/2019-cti-eu-bonding-eu-cyber-threat-intelligence>
- Colouring Outside the Lines (Andras Iklody & Trey Darley)
 - ▶ <https://www.first.org/conference/2020/recordings>
- MISP Training Materials
 - ▶ <https://github.com/MISP/misp-training>

2022-03-21

From evidences to actionable information
└ Conti ransomware group leak analysis
└ Acknowledgment

Provide sources along with the data!

- Turning data into actionable intelligence - advanced features in MISP supporting your analysts and tools (CIRCL.lu)
 - ▶ <https://www.enisa.europa.eu/events/2019-cti-eu/2019-cti-eu-bonding-eu-cyber-threat-intelligence>
- Colouring Outside the Lines (Andras Iklody & Trey Darley)
 - ▶ <https://www.first.org/conference/2020/recordings>
- MISP Training Materials
 - ▶ <https://github.com/MISP/misp-training>