MISP Project and ISACs

A versatile open source information sharing platform

Team CIRCL

TLP:WHITE

MISP Project

Who we are - MISP and CIRCL

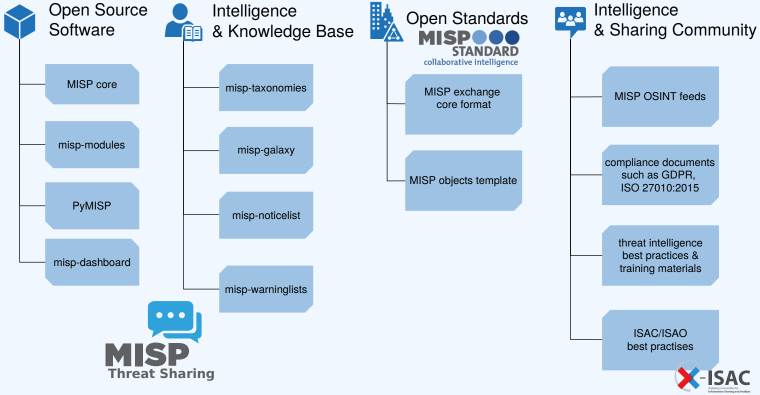
- CIRCL is mandated by the Ministry of Economy and acting as the Luxembourg National CERT for private sector.
- **CIRCL leads the development** of the Open Source MISP threat intelligence platform which is used by many military or intelligence communities, private companies, financial sector, National CERTs and LEAs globally.
- **CIRCL runs multiple large MISP communities performing active daily threat-intelligence sharing**.
- Funding is shared between Luxembourg, several European Union programs and partnerships (EU/US) agreements.

Plan

- An introduction to the MISP project and how it supports ISACs.
- Building an information sharing community, lessons learnt and best practices[1].

[1] We published the complete guidelines in `https://www.x-isac.org/assets/images/guidelines_to_set-up_an_ISAC.pdf`

MISP Project Overview



Open Source Software

- MISP core
- misp-modules
- PyMISP
- misp-dashboard

Intelligence & Knowledge Base

- misp-taxonomies
- misp-galaxy
- misp-noticelist
- misp-warninglists

Open Standards

- MISP exchange core format
- MISP objects template

Intelligence & Sharing Community

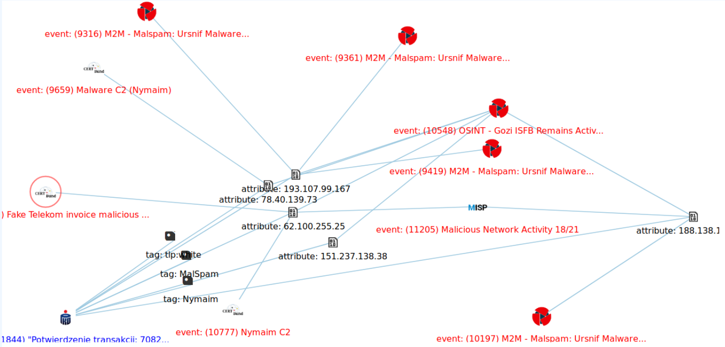
- MISP OSINT feeds
- compliance documents such as GDPR, ISO 27010:2015
- threat intelligence best practices & training materials
- ISAC/ISAO best practises

MISP features

- MISP project is an open source project developed the past 10-year with a large and active community.
- A complete set of features in MISP to work as a **threat intelligence platform** with a strong set of **information sharing capabilities**.
- A **flexible information sharing** model to support centralised, distributed or mixed model ISACs.
- Integration and extensability functionalities allow MISP to support different use-cases (from cybersecurity to complex intelligence community requirements).

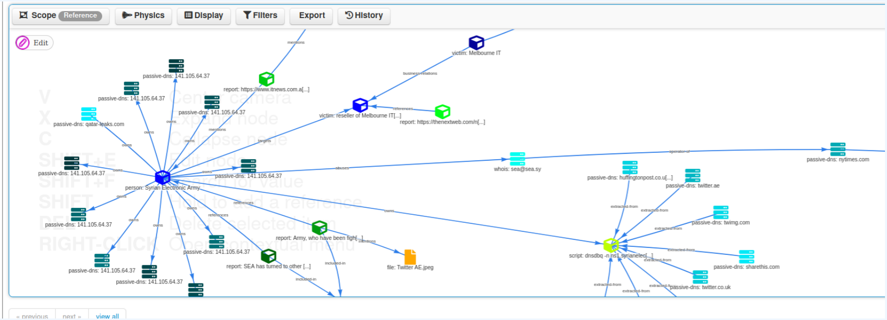
MISP FEATURE - CORRELATION

- MISP includes a **powerful engine for correlation** which allows analysts to discover correlating values between attributes.
- Getting a direct benefit from shared information by other ISAC members.


event: (9316) M2M - Malspam: Ursnif Malware...
event: (9361) M2M - Malspam: Ursnif Malware...
event: (9659) Malware C2 (Nymaim)
event: (10548) OSINT - Gozi ISFB Remains Activ...
event: (9419) M2M - Malspam: Ursnif Malware...
attribute: 193.107.99.167
attribute: 78.40.139.73
) Fake Telekom invoice malicious ...
MISP
attribute: 62.100.255.25
event: (11205) Malicious Network Activity 18/21
attribute: 188.138.1
attribute: 151.237.138.38
tag: tlp:white
tag: MalSpam
tag: Nymaim
event: (10777) Nymaim C2
1844) "Potwierdzenie transakcji: 7082...
event: (10197) M2M - Malspam: Ursnif Malware...

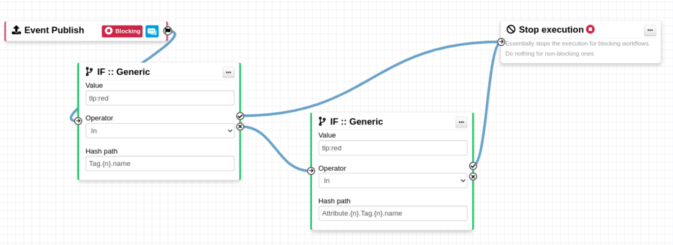
MISP feature - Event Graph

- **Analysts can create stories** based on graph relationships between objects, attributes.
- ISACs users can directly understand the information shared.


Scope
Reference
Physics
Display
Filters
Export
History
Edit
V Center camera
X Expand node
C Collapse node
SHIFT+E Edit node
SHIFT+F Search for value
SHIFT Hold to add a reference
DEL Delete selected item
RIGHT-CLICK Open contextual menu
mentions
victim: Melbourne IT
business-relations
passive-dns: 141.105.64.37
report: https://www.itnews.com.a[...]
passive-dns: 141.105.64.37
passive-dns: 141.105.64.37
victim: reseller of Melbourne IT[...]
references
report: https://thenextweb.com/n[...]
passive-dns: qatar-leaks.com
owns
mentions
targets
operator-of
passive-dns: nytimes.com
whois: sea@sea.sy
passive-dns: 141.105.64.37
abuses
passive-dns: 141.105.64.37
passive-dns: huffingtonpost.co.u[...]
passive-dns: twitter.ae
person: Syrian Electronic Army
references
extracted-from
passive-dns: twimg.com
passive-dns: 141.105.64.37
report: Army, who have been figh[...]
script: dnsdbq -n ns1.syrianelec[...]
passive-dns: 141.105.64.37
file: Twitter AE.jpeg
passive-dns: sharethis.com
report: SEA has turned to other [...]
included-in
passive-dns: 141.105.64.37
passive-dns: twitter.co.uk
passive-dns: 141.105.64.37
« previous
next »
view all

MISP FEATURE - WORKFLOW

- MISP can control publication steps via **customised workflow** when publishing events, creating new users...
- ISACs can enforce specific policies and rules via workflows.



Event Publish
Blocking

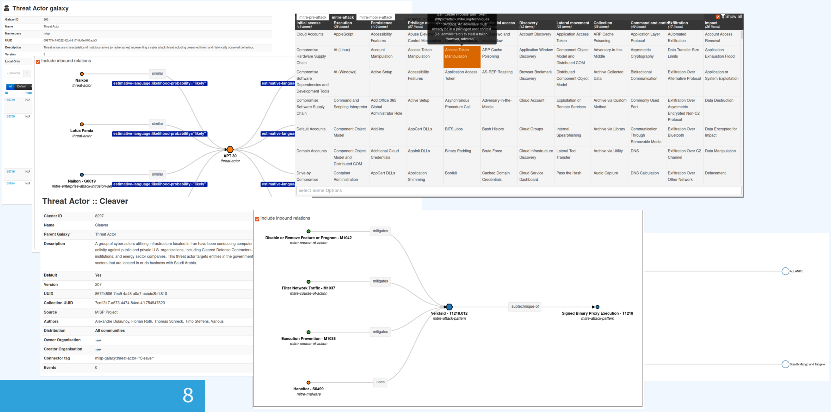
IF :: Generic
Value: tlp:red
Operator: In
Hash path: Tag.{n}.name

IF :: Generic
Value: tlp:red
Operator: In
Hash path: Attribute.{n}.Tag.{n}.name

Stop execution
Essentially stops the execution for blocking workflows.
Do nothing for non-blocking ones

MISP FEATURE - FLEXIBLE DATA MODELS

- MISP can be easily customised to support other data models (via **object templates, taxonomies and galaxies**).
- ISACs don’t need to change their models, policies or structure.
- A library of **290+ objects, 200+ taxonomies and many galaxies** (such as MITRE ATT&CK) are available.



Threat Actor galaxy

Galaxy ID	366
Name	Threat Actor
Namespace	misp
UUID	698774c7-8022-42c4-9171-8d6e4f06ada3
Description	Threat actors are characteristics of malicious actors (or adversaries) representing a cyber attack threat including presumed intent and historically observed behaviour.
Version	3
Local Only	

ID	Publ
165789	N/A
165769	N/A
165746	N/A
165894	N/A

☑ Include inbound relations

« previous
1
All
Default
Naikon
threat-actor
similar
estimative-language:likelihood-probability="likely"
Lotus Panda
threat-actor
similar
estimative-language:likelihood-probability="likely"
Naikon - G0019
mitre-enterprise-attack-intrusion-set
similar
estimative-language:likelihood-probability="likely"
APT 30
threat-actor
estimative-langua
estimative-langua
estimative-langua

Threat Actor :: Cleaver

Cluster ID	8297
Name	Cleaver
Parent Galaxy	Threat Actor
Description	A group of cyber actors utilizing infrastructure located in Iran have been conducting computer activity against public and private U.S. organizations, including Cleared Defense Contractors institutions, and energy sector companies. This threat actor targets entities in the government sectors that are located in or do business with Saudi Arabia.
Default	Yes
Version	207
UUID	86724806-7ec9-4a48-a0a7-ecbde3bf4810
Collection UUID	7cdff317-a673-4474-84ec-4f1754947823
Source	MISP Project
Authors	Alexandre Dulaunoy, Florian Roth, Thomas Schreck, Timo Steffens, Various
Distribution	All communities
Owner Organisation	MISP
Creator Organisation	MISP
Connector tag	misp-galaxy:threat-actor="Cleaver"
Events	0

Initial access (19 items)	Execution (38 items)	Persistence (110 items)	Privilege e (97 items)		Credential access	Discovery (42 items)	Lateral movement (23 items)	Collection (36 items)	Command and contr (40 items)	Exfiltration (17 items)	Impact (26 items)
Cloud Accounts	AppleScript	Accessibility Features	Abuse Elevation Control Mechanism	[illegible]	/etc/passwd and /etc/shadow	Account Discovery	Application Access Token	ARP Cache Poisoning	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Compromise Hardware Supply Chain	At (Linux)	Account Manipulation	Access Token Manipulation	Access Token Manipulation	ARP Cache Poisoning	Application Window Discovery	Component Object Model and Distributed COM	Adversary-in-the-Middle	Asymmetric Cryptography	Data Transfer Size Limits	Application Exhaustion Flood
Compromise Software Dependencies and Development Tools	At (Windows)	Active Setup	Accessibility Features	Application Access Token	AS-REP Roasting	Browser Bookmark Discovery	Distributed Component Object Model	Archive Collected Data	Bidirectional Communication	Exfiltration Over Alternative Protocol	Application or System Exploitation
Compromise Software Supply Chain	Command and Scripting Interpreter	Add Office 365 Global Administrator Role	Active Setup	Asynchronous Procedure Call	Adversary-in-the-Middle	Cloud Account	Exploitation of Remote Services	Archive via Custom Method	Commonly Used Port	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Data Destruction
Default Accounts	Component Object Model	Add-ins	AppCert DLLs	BITS Jobs	Bash History	Cloud Groups	Internal Spearphishing	Archive via Library	Communication Through Removable Media	Exfiltration Over Bluetooth	Data Encrypted for Impact
Domain Accounts	Component Object Model and Distributed COM	Additional Cloud Credentials	AppInit DLLs	Binary Padding	Brute Force	Cloud Infrastructure Discovery	Lateral Tool Transfer	Archive via Utility	DNS	Exfiltration Over C2 Channel	Data Manipulation
Drive-by Compromise	Container Administration	AppCert DLLs	Application Shimming	Bootkit	Cached Domain Credentials	Cloud Service Dashboard	Pass the Hash	Audio Capture	DNS Calculation	Exfiltration Over Other Network	Defacement

(i.e. [Create Process with Token](https://attack.mitre.org/techniques/T1134/002)). An adversary must already be in a privileged user context (i.e. administrator) to steal a token. However, adversa[...]

Select Some Options

☑ Include inbound relations

Communities operated by CIRCL

- As a CSIRT, CIRCL operates a wide range of communities
- We use it as an **internal tool** to cover various day-to-day activities
- Whilst being the main driving force behind the development, we're also one of the largest consumers
- Different communities have different needs and restrictions

Communities operated by CIRCL

- Private sector community
  - Our largest sharing community
  - Over **+1500 organisations**
  - **+4000 users**
  - Functions as a central hub for a lot of different sharing communities
  - Private organisations, researchers, various SoCs, some CSIRTs, etc
- CSIRT community
  - Tighter community
  - National CSIRTs, connections to international organisations, etc

Communities co-operated and supported by CIRCL

- Financial sector community
  - Banks, payment processors, etc.
  - Sharing of **mule accounts** and **non-cyber threat information**
- X-ISAC[2]
  - **Bridging the gap** between the various sectorial and geographical ISACs
  - New, but ambitious initiative
  - Goal is to **bootstrap the cross-sectorial sharing** along with building the infrastructure to enable sharing when needed

[2] https://www.x-isac.org/

Communities supported by CIRCL

- ISAC / specialised community MISPs
    - Topical or community specific instances hosted or co-managed by CIRCL
    - Examples, GSMA, FIRST.org, CSIRT network, PISAX.org, etc
    - Often come with their **own taxonomies and domain specific object definitions**
- FIRST.org's MISP community
- Telecom and Mobile operators' such as GSMA T-ISAC community
- Various ad-hoc communities for exercises for example
    - The ENISA exercise for example
    - Locked Shields exercise

Sharing Scenarios in MISP

- Sharing can happen for **many different reasons**. Let's see what we believe are the typical CSIRT scenarios
- We can generally split these activities into 4 main groups when we're talking about traditional CSIRT tasks:
  - Core services
  - Proactive services
  - Advanced services
  - Sharing communities managed by CSIRTs for various tasks

CSIRT core services

- Incident response
  - **Internal storage** of incident response data
  - Sharing of indicators **derived from incident response**
  - **Correlating data** derived and using the built in analysis tools
  - **Enrichment** services
  - **Collaboration** with affected parties via MISP during IR
  - **Co-ordination** and collaboration
  - **Takedown** requests
- Alerting of information leaks (integration with **AIL**[3])

[3] `https://www.ail-project.org/`

CSIRT proactive services

- **Contextualising** both internal and external data
- **Collection** and **dissimination** of data from various sources (including OSINT)
- Storing, correlating and sharing own manual research (**reversing, behavioural analysis**)
- Aggregating automated collection (**sandboxing, honeypots, spamtraps, sensors**)
  - MISP allows for the creation of **internal MISP "clouds"**
  - Store **large specialised datasets** (for example honeypot data)
  - MISP has **interactions with** a large set of such **tools** (Cuckoo, Mail2MISP, etc)
- **Situational awareness** tools to monitor trends and adversary TTPs within my sector/geographical region (MISP-dashboard, built in statistics)

CSIRT advanced services

- Supporting **forensic analysts**
- Collaboration with **law enforcement**
- **Vulnerability** information sharing
    - **Notifications** to the constituency about relevant vulnerabilities
    - **Co-ordinating** with vendors for notifications (*)
    - Internal / closed community sharing of pentest results

ISACs and CSIRT role in information sharing

- **Reporting** non-identifying information about incidents (such as outlined in NISD)
- **Seeking** and engaging in **collaboration** with CSIRT or other parties during an incident
- Pre-sharing information to **request for help** / additional information from the community
- **Pseudo-anonymised sharing** through 3rd parties to **avoid attribution** of a potential target
- Building processes for **other types of sharing** to get the community engaged and acquainted with the methodologies of sharing (mule account information, disinformation campaigns, border control, etc)

Compliance, legal framework and ISACs

- MISP project collaborated with legal advisory services
  - Information sharing and cooperation **enabled by GDPR**;
  - How MISP enables stakeholders identified by the **NISD** to perform key activities;
  - **ISO/IEC 27010:2015** - Information security management for inter-sector and inter-organizational communications;
  - Guidelines to setting up an information sharing community such as an ISAC or ISAO;
- For more information: https://www.misp-project.org/compliance/

Getting started with building your own sharing community

- Starting a sharing community is **both easy and difficult** at the same time
- Many moving parts and most importantly, you'll be dealing with a **diverse group of people**
- Understanding and working with your constituents to help them face their challenges is key

Running a sharing community using MISP - How to get going?

- Different models for constituents
  - **Connecting to** a MISP instance hosted by a ISAC
  - **Hosting** their own instance and connecting to ISAC's MISP
  - **Becoming member** of a sectorial MISP community that is connected to ISAC's community
- Planning ahead for future growth
  - Estimating requirements
  - Deciding early on common vocabularies
  - Offering services through MISP

Rely on our instincts to immitate over expecting adherence to rules

- **Lead by example** - the power of immitation
- Encourage **improving by doing** instead of blocking sharing with unrealistic quality controls
  - What should the information look like?
  - How should it be contextualise
  - What do you consider as useful information?
  - What tools did you use to get your conclusions?
  - How the information could be used by the ISAC members?
- Side effect is that you will end up **raising the capabilities of your constituents**

What counts as valuable data?

- Sharing comes in many shapes and sizes
  - Sharing results / reports is the classical example
  - Sharing enhancements to existing data
  - Validating data / flagging false positives
  - Asking for support from the community
- **Embrace all of them**. Even the ones that don't make sense right now, you never know when they come handy...

How to deal with organisations that only "leech"?

- From our own communities, only about **30%** of the organisations **actively share data**
- We have come across some communities with sharing requirements
- In our experience, this sets you up for failure because:
  - Organisations losing access are the ones who would possibily benefit the most from it
  - Organisations that want to stay above the thresholds will start sharing junk / fake data
  - You lose organisations that might turn into valuable contributors in the future

So how does one convert the passive organisations into actively sharing ones?

- Rely on **organic growth** and it takes time (+2 years is common)
- **Help** them increase their capabilities
- As mentioned before, lead by example
- Rely on the inherent value to one's self when sharing information (validation, enrichments, correlations)
- **Give credit** where credit is due, never steal the contributions of your community (that is incredibly demotivating)

Dispelling the myths around blockers when it comes to information sharing

- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
  - You can play a role here: organise regular workshops, conferences, have face to face meetings
- Legal restrictions
  - "Our legal framework doesn't allow us to share information."
  - "Risk of information leak is too high and it's too risky for our organization or partners."
- Practical restrictions
  - "We don't have information to share."
  - "We don't have time to process or contribute indicators."
  - "Our model of classification doesn't fit your model."
  - "Tools for sharing information are tied to a specific format, we use a different one."

Contextualising the information

- Sharing **technical information** is a **great start**
- However, to truly create valueable information for your community, always consider the context:
  - Your IDS might not care why it should alert on a rule
  - But your analysts will be interested in the threat landscape and the "big picture"
- Classify data to make sure your partners understand why it is **important for you**, so they can see why it could be **useful to them**
- Massively important once an organisation has the maturity to filter the most critical **subsets of information for their own defense**

Choice of vocabularies

- MISP has a verify **versatile system** (taxonomies) for classifying and marking data
- However, this includes different vocabularies with obvious overlaps
- MISP allows you to **pick and choose vocabularies** to use and enforce in a community
- Good idea to start with this process early
- If you don't find what you're looking for:
  - Create your own (JSON format, no coding skills required)
  - If it makes sense, share it with us via a pull request for redistribution

Conclusion

- MISP is a complete and advanced open source stack available to create large international sharing communities (JP/US/EU).
- Building and improving ISACs is critical to limit the impact of security threats.
- We welcome partnerships in the field of information sharing.

Get in touch if you need some help to get started

- Getting started with building a new community can be daunting. Feel free to get in touch with us if you have any questions!
- Contact: info@circl.lu
- `https://www.circl.lu/`
- `https://github.com/MISP`
  `https://www.misp-project.org/`
  `https://twitter.com/MISPProject`

Backup slides

Backup slides

Shared libraries of meta-information (Galaxies)

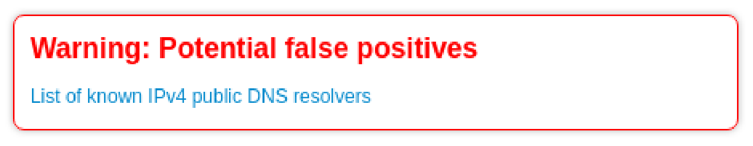
- The MISPProject in co-operation with partners provides a **curated list of galaxy information**
- Can include information packages of different types, for example:
  - Threat actor information (event different models or approaches)
  - Specialised information such as Ransomware, Exploit kits, etc
  - Methodology information such as preventative actions
  - Classification systems for methodologies used by adversaries - ATT&CK
- Consider improving the default libraries or contributing your own (simple JSON format)
- If there is something you cannot share, run your own galaxies and **share it out of bound** with partners
- Pull requests are always welcome

False-positive handling

- You might often fall into the trap of discarding seemingly "junk" data
- Besides volume limitations (which are absolutely valid, fear of false-positives is the most common reason why people discard data) - Our recommendation:
  - Be lenient when considering what to keep
  - Be strict when you are feeding tools
- MISP allows you to **filter out the relevant data on demand** when feeding protective tools
- What may seem like **junk to you may** be absolutely **critical to other users**

False-positive handling

- **Analysts** will often be interested in the **modus operandi** of threat actors over **long periods of time**
- Even cleaned up infected hosts might become interesting again (embedded in code, recurring reuse)
- Use the tools provided to eliminate obvious false positives instead and limit your data-set to the most relevant sets



Warning: Potential false positives

List of known IPv4 public DNS resolvers