

Threat Intelligence and Information Sharing

PISAX.org - MISP introduction training

Alexandre Dulaunoy

MISP Project

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

PISAX.org Online Training



MISP
Threat Sharing

- (14:00 - 15:00) Introduction to Information Sharing with MISIP
- (15:00 - 15:20) Quick demo of the PISAX.org threat sharing platform
- (15:20 - 16:00) Interactive session with the IXPs community

- During a malware analysis workgroup in 2012, we discovered that we worked on the analysis of the same malware.
- We wanted to share information in an easy and automated way **to avoid duplication of work.**
- Christophe Vandeplass (then working at the CERT for the Belgian MoD) showed us his work on a platform that later became MISP.
- A first version of the MISP Platform was used by the MALWG and **the increasing feedback of users** helped us to build an improved platform.
- MISP is now **a community-driven development.**

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

- 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.**



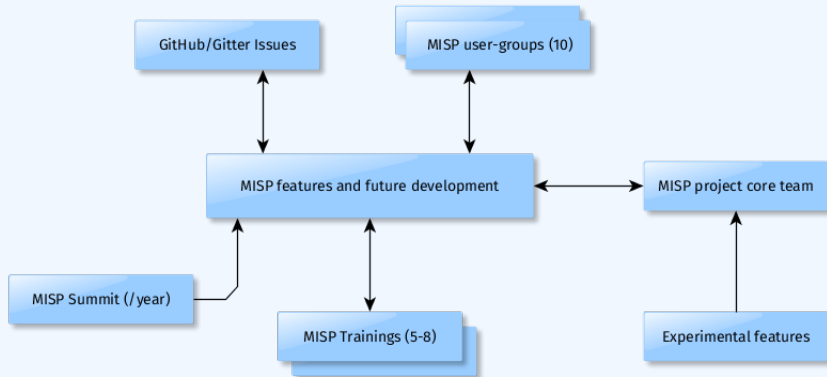
Co-financed by the European Union

Connecting Europe Facility

- PISAX stands for "Pan-European Information Sharing and Analysis for Internet Exchange Point and Global Roaming Exchange". The overall objective of this action is to create a common Information Sharing and Analysis Center (ISAC) to support Internet Exchange Points (IXPs) and General Packet Radio Service Roaming eXchange (GRXs) at the national, European and international level.
- PISAX will provide an automated and secure threat intelligence sharing system building on the existing MISP threat intelligence platform hence allowing IXPs and GRXs to improve their current security posture.

- There are many different types of users of an information sharing platform like MISP:
 - ▶ **Malware reversers** willing to share indicators of analysis with respective colleagues.
 - ▶ **Security analysts** searching, validating and using indicators in operational security.
 - ▶ **Intelligence analysts** gathering information about specific adversary groups.
 - ▶ **Law-enforcement** relying on indicators to support or bootstrap their DFIR cases.
 - ▶ **Risk analysis teams** willing to know about the new threats, likelihood and occurrences.
 - ▶ **Fraud analysts** willing to share financial indicators to detect financial frauds.
 - ▶ **Telecom** community sharing information at large.

MISP MODEL OF GOVERNANCE



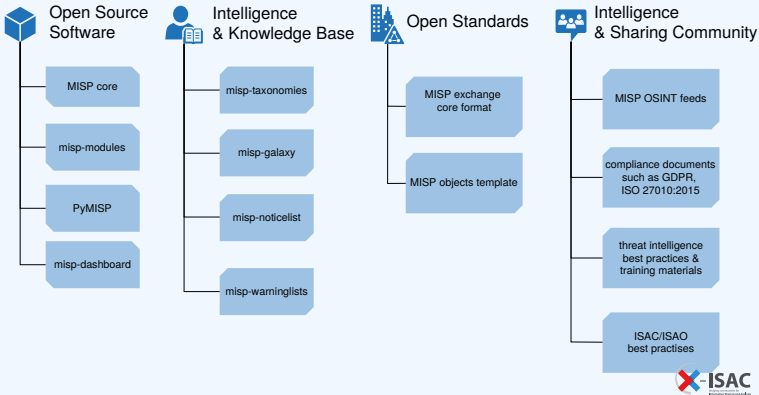
MANY OBJECTIVES FROM DIFFERENT USER-GROUPS

- Sharing indicators for a **detection** matter.
 - ▶ 'Do I have infected systems in my infrastructure or the ones I operate?'
- Sharing indicators to **block**.
 - ▶ 'I use these attributes to block, sinkhole or divert traffic.'
- Sharing indicators to **perform intelligence**.
 - ▶ 'Gathering information about campaigns and attacks. Are they related? Who is targeting me? Who are the adversaries?'
- → These objectives can be conflicting (e.g. False-positives have different impacts)

- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
- Legal restriction¹
 - ▶ "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 restriction
 - ▶ "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."

¹<https://www.misp-project.org/compliance/>

MISP PROJECT OVERVIEW

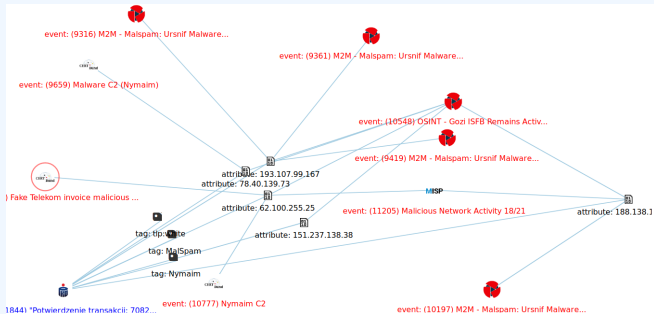


- MISP² is a threat information sharing free & open source software.
- MISP has **a host of functionalities** that assist users in creating, collaborating & sharing threat information - e.g. flexible sharing groups, **automatic correlation**, free-text import helper, event distribution & proposals.
- Many export formats which support IDses / IPses (e.g. Suricata, Bro, Snort), SIEMs (eg CEF), Host scanners (e.g. OpenIOC, STIX, CSV, yara), analysis tools (e.g. Maltego), DNS policies (e.g. RPZ).
- A rich set of MISP modules³ to add expansion, import and export functionalities.

²<https://github.com/MISP/MISP>

³<https://www.github.com/MISP/misp-modules>

CORRELATION FEATURES: A TOOL FOR ANALYSTS

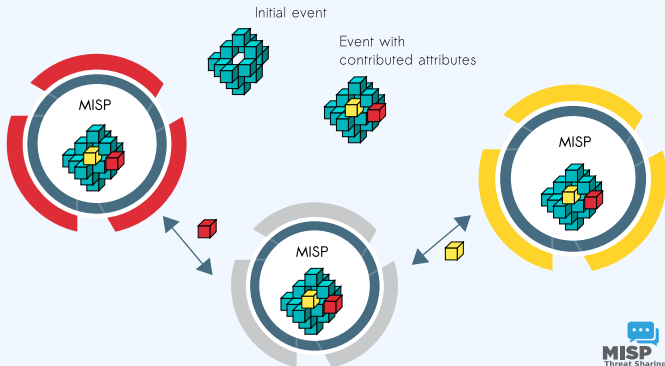


- To **corroborate a finding** (e.g. is this the same campaign?), **reinforce an analysis** (e.g. do other analysts have the same hypothesis?), **confirm a specific aspect** (e.g. are the sinkhole IP addresses used for one campaign?) or just find if this **threat is new or unknown in your community.**

- Communities are groups of users sharing within a set of common objectives/values.
- CIRCL operates multiple MISP instances with a significant user base (more than 950 organizations with more than 2400 users).
- **Trusted groups** running MISP communities in island mode (air gapped system) or partially connected mode.
- **Financial sector** (banks, ISACs, payment processing organizations) use MISP as a sharing mechanism.
- **Military and international organizations** (NATO, military CSIRTs, n/g CERTs,...).
- **Security vendors** running their own communities (e.g. Fidelis) or interfacing with MISP communities (e.g. OTX).

MISP CORE DISTRIBUTED SHARING FUNCTIONALITY

- MISPs' core functionality is sharing where everyone can be a consumer and/or a contributor/producer."
- Quick benefit without the obligation to contribute.
- Low barrier access to get acquainted to the system.



EVENTS, OBJECTS AND ATTRIBUTES IN MISP

- MISP events are encapsulations for contextually linked information
- MISP attributes⁴ initially started with a standard set of "cyber security" indicators.
- MISP attributes are purely **based on usage** (what people and organizations use daily).
- Evolution of MISP attributes is based on practical usage & users (e.g. the addition of **financial indicators** in 2.4).
- MISP objects are attribute compositions describing points of data using many facets, constructed along the lines of community and user defined templates.
- Galaxies granularly contextualise, classify & categorise data based on **threat actors, preventive measures**, tools used by adversaries.

⁴attributes can be anything that helps describe the intent of the event package from indicators, vulnerabilities or any relevant information

- Indicators⁵
 - ▶ Indicators contain a pattern that can be used to detect suspicious or malicious cyber activity.
- Attributes in MISP can be network indicators (e.g. IP address), system indicators (e.g. a string in memory) or even bank account details.
 - ▶ **A type (e.g. MD5, url) is how an attribute is described.**
 - ▶ An attribute is always in a category (e.g. Payload delivery) which puts it in a context.
 - **A category is what describes** an attribute.
 - ▶ An IDS flag on an attribute allows to determine if **an attribute can be automatically used for detection.**

⁵IoC (Indicator of Compromise) is a subset of indicators

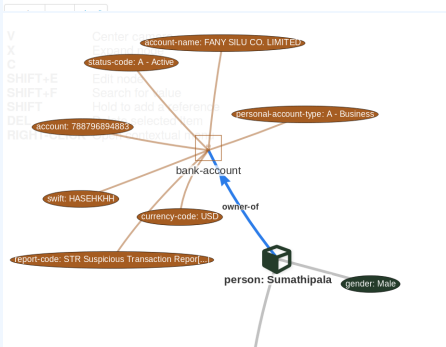
SHARING ATTACKERS TECHNIQUES

- MISP integrates at event or attribute level MITRE's Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK).

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	Secured 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 Shimring	Rootkit	Bash History	Process Discovery	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 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_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 Doppelgänger	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

SUPPORTING SPECIFIC DATAMODEL

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
2018-09-28			bank-account						
Name: bank-account									
References: 0									
2018-09-28		Other	status-code:	A - Active		Add			
2018-09-28		Other	report-code:	STR Suspicious Transaction Report		Add			
2018-09-28		Other	personal-account-type:	A - Business		Add			
2018-09-28		Financial fraud	swift:	HASEHKHH		Add		<input checked="" type="checkbox"/>	3849 11320 11584
2018-09-28		Financial fraud	account:	788796894883		Add		<input checked="" type="checkbox"/>	
2018-09-28		Other	account-name:	FANY SILU CO. LIMITED		Add		<input checked="" type="checkbox"/>	
2018-09-28		Other	currency-code:	USD		Add			



- Contributors can use the UI, API or using the freetext import to add events and attributes.
 - ▶ Modules existing in Viper (a binary framework for malware reverser) to populate and use MISP from the vty or via your IDA.
- Contribution can be direct by creating an event but **users can propose attributes updates** to the event owner.
- **Users should not be forced to use a single interface to contribute.**

EXAMPLE: FREETEXT IMPORT IN MISP









Freetext Import Tool

Paste a list of IOCs into the field below for automatic detection.

This is a sample text to show how indicators can be extracted. Just paste your text including indicators such as 23.100.122.175, host.microsoft.com, or b447c27a00e3a348881b0030177000cd in here and the tool will automatically detect the indicators and save them as attributes - after allowing you to make some last minute changes. For more information, visit <https://www.github.com/MISP/MISP>









Freetext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

Value	Category	Type	IDS	Comment	Actions
23.100.122.175	Network activity	ip-dst	<input checked="" type="checkbox"/>	Imported via the freetext import.	 
host.microsoft.com	Network activity	hostname	<input checked="" type="checkbox"/>	Imported via the freetext import.	 
b447c27a00e3a348881b0030177000cd	Payload delivery	md5	<input checked="" type="checkbox"/>	Imported via the freetext import.	 
https://www.github.com/MISP/MISP	Network activity	url	<input checked="" type="checkbox"/>	Imported via the freetext import.	 

ip-dst → ip-src

Update all comment fields

		Filters: All File Network Financial Proposal Correlation									
Date	Org	Category	Type	Value	Comment	Related Events	IDS	Distribution	Actions		
2016-02-24		Network activity	hostname	host.microsoft.com	Imported via the freetext import.		Yes	Inherit	 		
2016-02-24		Network activity	ip-dst	23.100.122.175	Imported via the freetext import.	298	Yes	Inherit	 		
2016-02-24		Network activity	url	https://www.github.com/MISP/MISP	Imported via the freetext import.		Yes	Inherit	 		
2016-02-24		Payload delivery	md5	b447c27a00e3a348881b0030177000cd	Imported via the freetext import.		Yes	Inherit	 		

SUPPORTING CLASSIFICATION

- Tagging is a simple way to attach a classification to an event or an attribute.
- **Classification must be globally used to be efficient.**
- MISP includes a flexible tagging scheme where users can select from more than 42 existing taxonomies or create their own taxonomy.

18	✓	✗	admiralty-scale:information-credibility--"1"	admiralty-scale	4	0		<input type="checkbox"/>		
19	✓	✗	admiralty-scale:information-credibility--"2"	admiralty-scale	15	1		<input type="checkbox"/>		
20	✓	✗	admiralty-scale:information-credibility--"3"	admiralty-scale	12	4		<input type="checkbox"/>		
21	✓	✗	admiralty-scale:information-credibility--"4"	admiralty-scale	1	0		<input type="checkbox"/>		
22	✓	✗	admiralty-scale:information-credibility--"5"	admiralty-scale	1	0		<input type="checkbox"/>		
23	✓	✗	admiralty-scale:information-credibility--"3"	admiralty-scale	2	0		<input type="checkbox"/>		
12	✓	✗	admiralty-scale:source-reliability--"a"	admiralty-scale	0	0		<input type="checkbox"/>		
13	✓	✗	admiralty-scale:source-reliability--"b"	admiralty-scale	15	53		<input type="checkbox"/>		
14	✓	✗	admiralty-scale:source-reliability--"c"	admiralty-scale	5	2		<input type="checkbox"/>		
15	✓	✗	admiralty-scale:source-reliability--"d"	admiralty-scale	1	0		<input type="checkbox"/>		
16	✓	✗	admiralty-scale:source-reliability--"a"	admiralty-scale	0	0		<input type="checkbox"/>		
17	✓	✗	admiralty-scale:source-reliability--"1"	admiralty-scale	4	2		<input type="checkbox"/>		
1203	✓	✗	adversary:infrastructure-action--"monitoring-active"	adversary	1	0		<input type="checkbox"/>		
1201	✓	✗	adversary:infrastructure-action--"passive-only"	adversary	0	0		<input type="checkbox"/>		

- Delegate events publication to another organization (introduced in MISP 2.4.18).
 - ▶ The other organization can take over the ownership of an event and provide **pseudo-anonymity to initial organization**.
- Sharing groups allow custom sharing (introduced in MISP 2.4) per event or even at attribute level.
 - ▶ Sharing communities can be used locally or even cross MISP instances.
 - ▶ **Sharing groups** can be done at **event level or attributes level** (e.g. financial indicators shared to a financial sharing groups and cyber security indicators to CSIRT community).

The screenshot displays the MISP interface for an event. At the top, there is a table of events with columns for checkboxes, status, and actions. A tooltip for 'Sightings' is shown over the first event, indicating 'CIRCL: 2 (2017-03-19 16:17:59)'. Below the event, the 'Sighting Details' section shows 'No' sightings, with a red bar indicating this status. The 'Discussion' section is also visible.

Events			
<input checked="" type="checkbox"/>	No	Sightings CIRCL: 2 (2017-03-19 16:17:59)	
<input checked="" type="checkbox"/>	No	(2/0/0)	
<input checked="" type="checkbox"/>	No	Inherit	

Tags **+**

Date 2016-02-24

Threat Level High

Analysis Initial

Distribution Connected communities

freetext test

Sighting Details **No**

MISP: 2 4 (2) - restricted to own organisation only.

CIRCL: 2

Discussion

- Sightings allow users to notify the community about the activities related to an indicator.
- In recent MISP versions, the sighting system supports negative sightings (FP) and expiration sightings.
- Sightings can be performed via the API, and the UI, even including the import of STIX sighting documents.
- Many use-cases for scoring indicators based on users sighting.

- False-positives are a recurring challenge in information sharing.
- In MISP 2.4.39, we introduced the `misp-warninglists`⁶ to help analysts in their day-to-day job.
- Predefined lists of well-known indicators which are often false-positives like RFC1918 networks, public DNS resolver are included by default.

⁶<https://github.com/MISP/misp-warninglists>

IMPROVING SUPPORT OF SHARING WITHIN AND OUTSIDE AN ORGANIZATION

- Even in a single organization, multiple use-cases of MISP can appear (groups using it for dynamic malware analysis correlations, dispatching notification).
- In MISP 2.4.51, we introduced the ability to have **local MISP** servers connectivity to avoid changes in distribution level. This allows to have mixed synchronization setup within and outside an organization.
- Feed support was also introduced to support synchronization between untrusted and trusted networks.

- We maintain the default CIRCL OSINT feeds (TLP:WHITE selected from our communities) in MISP to allow users to ease their bootstrapping.
- The format of the OSINT feed is based on standard MISP JSON output pulled from a remote TLS/HTTP server.
- Additional content providers can provide their own MISP feeds. (<https://botvrij.eu/>)
- Allows users to **test their MISP installations and synchronisation with a real dataset.**
- Opening contribution to other threat intel feeds but also allowing the analysis of overlapping data⁷.

⁷A recurring challenge in information sharing

- **Information sharing practices come from usage** and by example (e.g. learning by imitation from the shared information).
- MISP is just a tool. What matters is your sharing practices. The tool should be as transparent as possible to support you.
- Enable users to customize MISP to meet their community's use-cases (e.g. gathering ideas and feedback within PISAX.org community).
- MISP project combines open source software, open standards, best practices and communities to make information sharing a reality.