Improving Intelligence Community

MISP as an enabler for intelligence analysis

MISP Project
https://www.misp-project.org/

20181117

MISP
Threat Sharing

Alexandre Dulaunoy @adulau @MISPProject

MISP and CIRCL

- CIRCL is mandated by the Ministry of Economy and acting as the Luxembourgish National CERT for private sector.
- CIRCL leads the development of the Open Source MISP threat intelligence platform which is used by a wide range of military or intelligence communities, private companies, the 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

MISP Project

MISP Project is a **completely open collaborative effort** to support analysts and organisations in all efforts related to **information sharing and threat intelligence**.
The project includes a range of open source software, composed of a **threat intelligence platform** with sharing capabilities, expansion modules, advanced API capabilities and situational awareness tools.
It also includes a comprehensive intelligence library and knowledge base acting as reference material for common taxonomies and classifications, threat-actors, complex intelligence models and common false-positive warning libraries.
Furthermore, the project encompasses a set of **open standards**, of which the reference implementation is MISP itself, designed to be freely reused by communities developing their own software and tools.
In addition, the MISP project releases a set of best practises that can be used as guidelines meant **to support closed, semi-open and open sharing communities**.

MISP Threat Sharing

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

X-ISAC

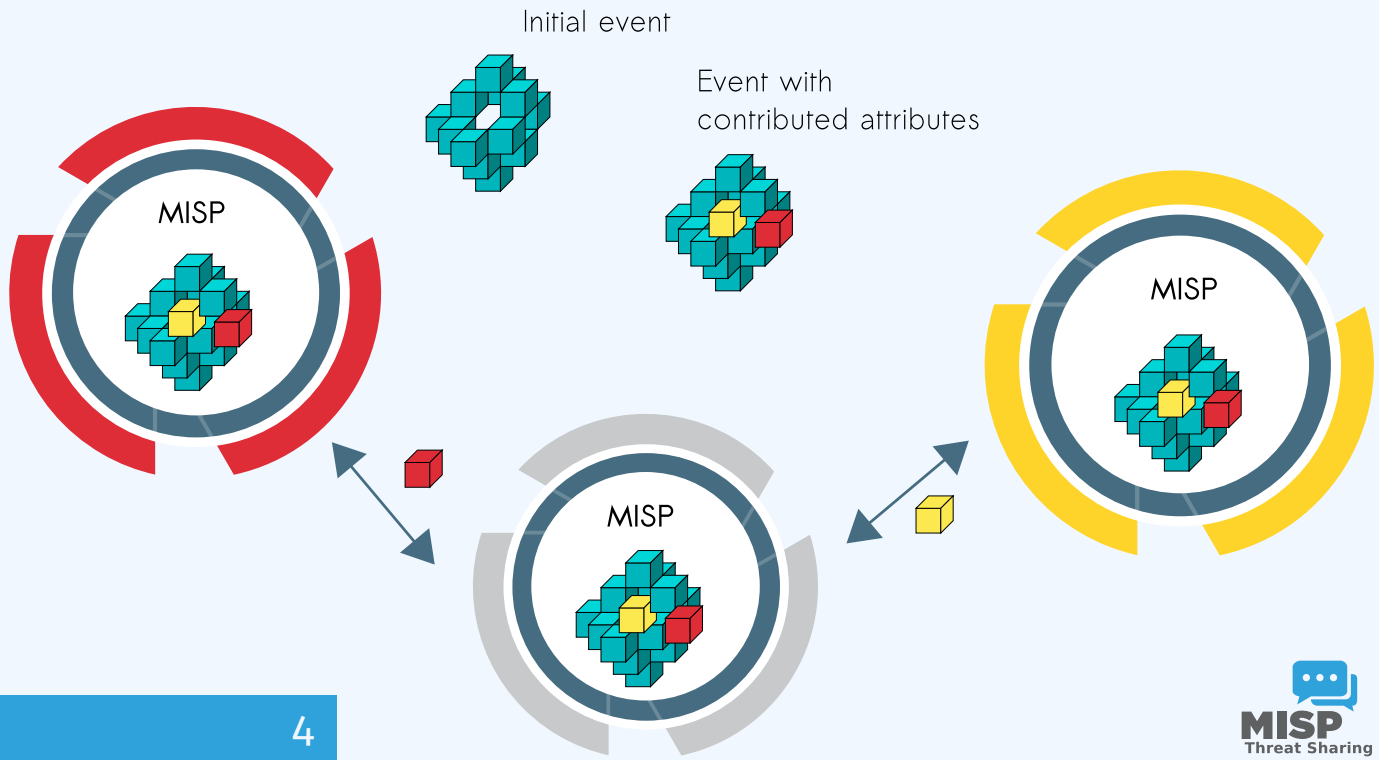
MISP features

- MISP[1] 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, sigma), analysis tools (e.g. Maltego), DNS policies (e.g. RPZ).
- A rich set of MISP modules[2] to add expansion, import and export functionalities. A strong integration with other open source security projects such as **TheHive**, **Cortex**, cve-search, **AIL framework**.

[1] https://github.com/MISP/MISP
[2] https://www.github.com/MISP/misp-modules

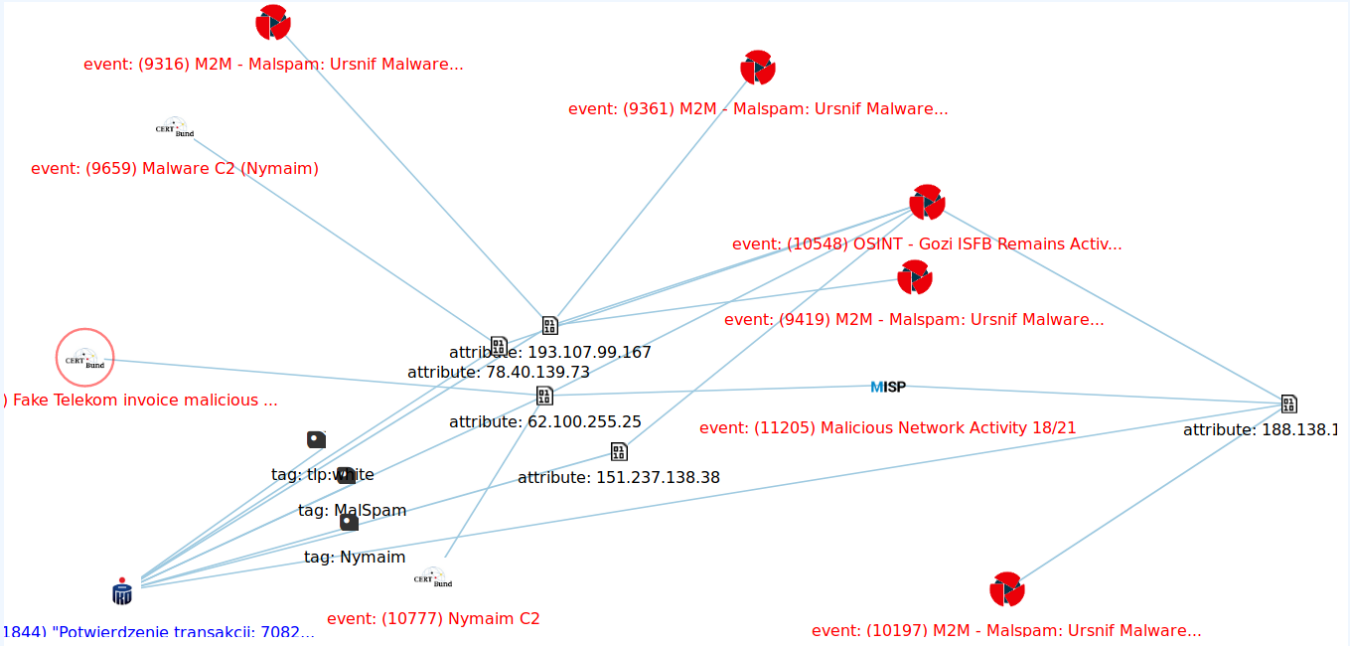
MISP CORE DISTRIBUTED SHARING FUNCTIONALITY

- MISPs' core functionality is sharing where everyone can be a consumer and/or a contributor/producer."
- Starting a sharing community by installing MISP is simple and then you can synchronised with any other sharing community using MISP.
- Contributions can be done via proposals, sightings or extending events.



MISP Threat Sharing

Correlation features: a tool for analysts

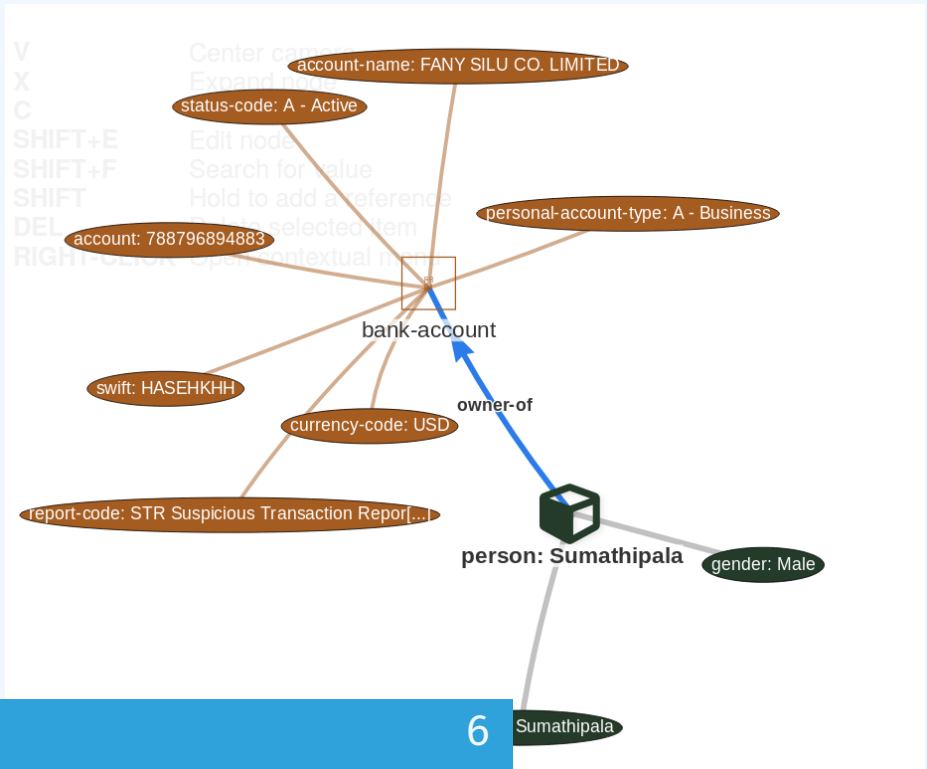


- To **corroborate a finding** (e.g. is this the same campaign?), **reinforce an analysis** (e.g. do other analysts have the same hypothesis?), **confirm specific aspects** (e.g. are the sinkhole IP addresses used for one campaign?) or just find whether the given **threat is new or unknown in your community**.

Supporting custom shareable datamodels

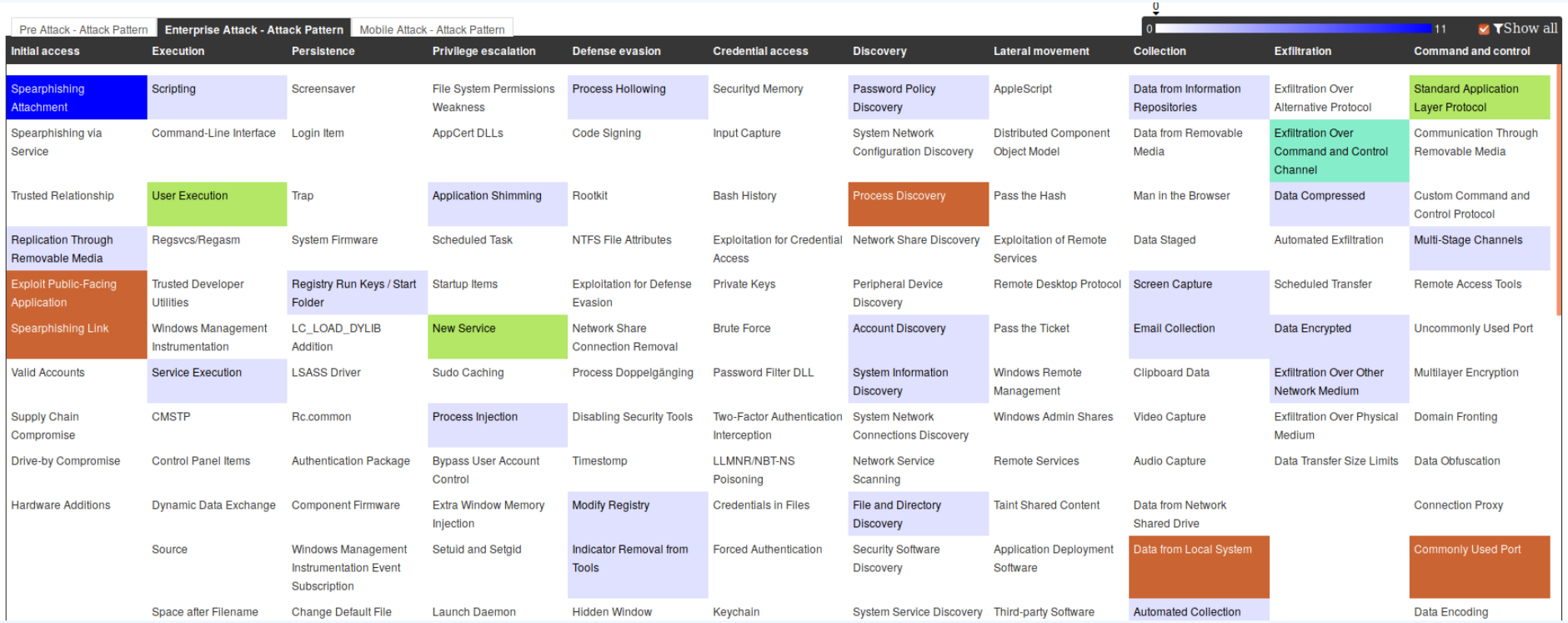
Filters: All | File | Network | Financial | Proposal | Correlation | Warnings | Include deleted attributes | Show context fields

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events
2018-09-28		**Name:** bank-account **References:** 0							
2018-09-28		Other	**status-code:** text	A - Active	+	Add		☐	
2018-09-28		Other	**report-code:** text	STR Suspicious Transaction Report	+	Add		☐	
2018-09-28		Other	**personal-account-type:** text	A - Business	+	Add		☐	
2018-09-28		Financial fraud	**swift:** bic	HASEHKHH	+	Add		☑	3849 11320 11584
2018-09-28		Financial fraud	**account:** bank-account-nr	788796894883	+	Add		☑	
2018-09-28		Other	**account-name:** text	FANY SILU CO. LIMITED	+	Add		☑	
2018-09-28		Other	**currency-code:** text	USD	+	Add		☐	



Sharing Attackers Techniques

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



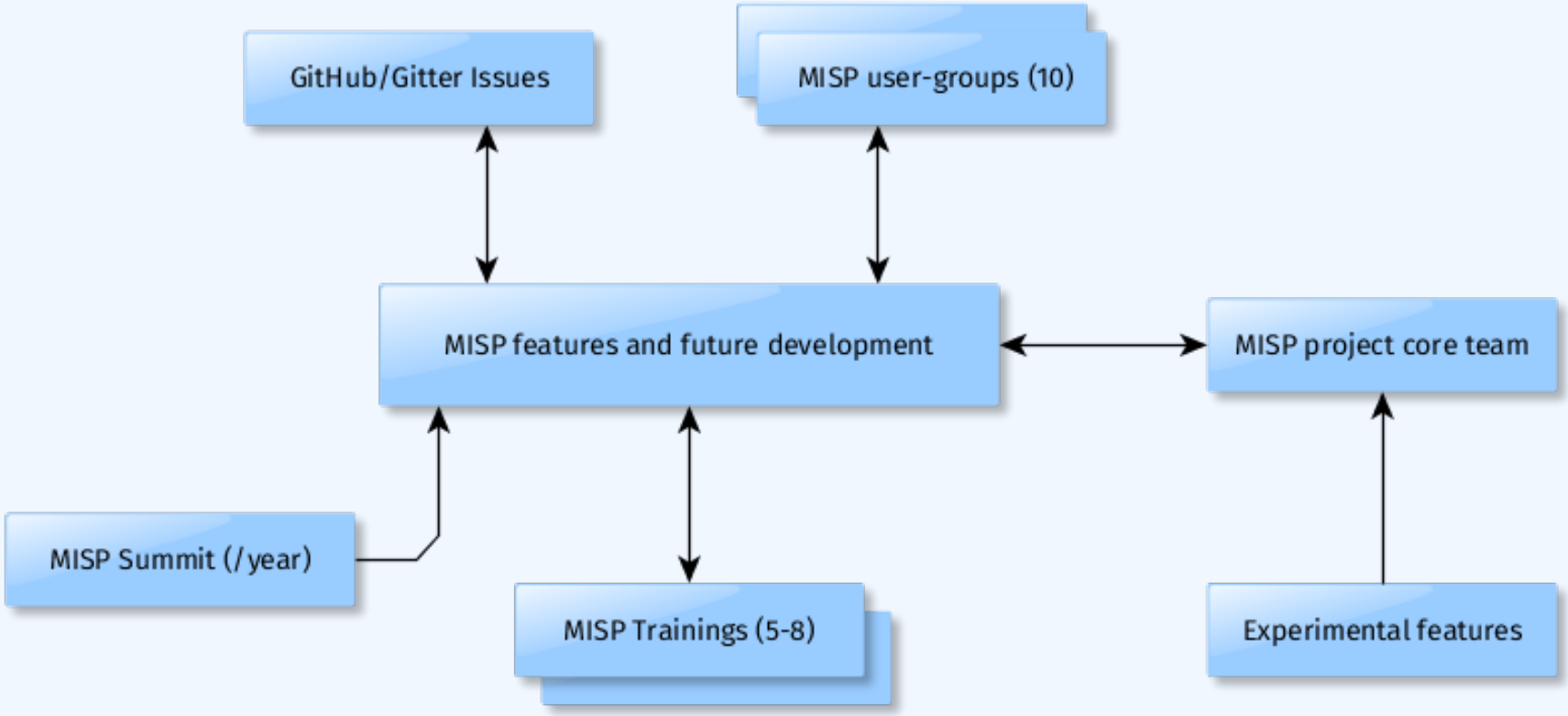
Pre Attack - Attack Pattern | **Enterprise Attack - Attack Pattern** | Mobile Attack - Attack Pattern

0 — 11 — Show all

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	Exfiltration	Command and control
Spearphishing Attachment	Scripting	Screensaver	File System Permissions Weakness	Process Hollowing	Securityd Memory	Password Policy Discovery	AppleScript	Data from Information Repositories	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	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 Doppelgänging	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	Timestomp	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

When and where did the intelligence community become involved?

MISP MODEL OF GOVERNANCE



PMF methodology

[3]

[3] https://github.com/adulau/pmf

New users and use-cases in MISP

- There are many different types of users of MISP such as Malware reversers, incident responders, security analysts, intelligence analysts, LEAs, fraud and financial analysts (from 2012 until Today).
- **IC community is not an island**. They evaluated the ability to gather information from other sharing communities and in some cases even **buildt their own internal community**[4].

[4] MISP is designed to support various models such as disconnected sharing communities (e.g. military air-gapped ones), partially bridged or fully interconnected communities

Secrecy in IC

- Secrecy of Methodologies
- Secrecy of Tools used
- Information Secrecy

But finding the trade-off between secrecy and efficacy is hard and very often secrecy beats efficacy[5].

[5] *Analytic Culture in the US Intelligence Community: An Ethnographic Study. Dr. Rob Johnston*

Social and political aspects

- a part of the secrecy (in methodologies), tooling decision or lack of information sharing is often linked to political or social aspects:

> Here in the CJOC we have eight different computer systems.... And there is no compatibility. So information needs to be transferred manually.... The United States use SIPR to the tactical level. The SIPR terminal is located in a separate room. So when information needs to be transmitted, a U.S. officer needs to manually write down the information, walk to the other room, and then insert the information in an ISAF [SECRET] system....[This] hampers troops at the tactical level.... There are no barriers to information sharing at the tactical level, because at the tactical level lives are at stake. At the operational level,... politics come in. National agendas.... And these...agendas are sometimes conflicting. So governments prohibit information to be shared [and] systems to be compatible. [6]

[6] Information Sharing in Military Organizations: A Sociomaterial Perspective, Gijs Van den Heuvel

Complexity, efficacy and secrecy

Secrecy and efficacy conflict. Secrecy interferes with analytic effectiveness by limiting access to information and sources that may be necessary for accurate or predictive analysis[7]

- OSINT increased in IC and takes a significant role in analytics nowadays.
- Purely open models where secrecy is limited (information is disclosed along with tools and methodologies used) such as bellingcat[8] or the systematic work of Pieter Van Ostaeyen[9] can be very efficient.

[7] Analytic Culture in the US Intelligence Community: An Ethnographic Study. Dr. Rob Johnston

[8] `https://www.bellingcat.com/`

[9] Tracking ISIS

Sharing with potential hostile forces

Information sharing among hostile forces is a different game, although it has been argued that, even among enemies, information sharing about their mutual strengths and intentions is conducive to preventing conflicts from occurring. Stated the other way around, military secrecy may stimulate violent encounters[10][11]

- Large sharing communities might contain some hostile adversaries but often the sharing aspect outperforms the risk(s).

[10] Parks, W. (1957). Secrecy and the public interest in military affairs. George Washington Law Review, 23-27.

[11] Coser, L. (1963). The dysfunctions of military secrecy. Social Problems, 11(1),13-22.

Sharing to support collaborative analysis

Finally, the main problem of intelligence gathering seems not to be the sharing, but information credibility, which is nevertheless also linked to information exchange. To verify the credibility of information, crosschecking is essential and this task implies sharing with others.[12]

- Extensive taxonomies in estimative language(s) supports the crosschecking role of the analyst.
- Interoperable standard (such as MISP core exchange format and MISP) can improve the sharing aspect inter-agencies.

[12] Information Sharing Among Military Operational Staff: The French Officers' Experience, Barbara Jankowski

Conclusion

- **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. **IC community and threat intelligence community can both learn from each others**.
- MISP project combines open source software, open standards, best practices and communities to make information sharing a reality.

Contact

- Getting started with building a new community can be daunting or want to provide feedback about MISP, don't hesitate to contact us:
- Contact: info@circl.lu - info@misp-project.org
- `https://www.circl.lu/`
- `https://github.com/MISP` - `https://twitter.com/MISPProject`
- `https://github.com/CIRCL`

Co-financed by the European Union

Connecting Europe Facility

Some "not so funny" examples of the information sharing challenges in the military and IC.

coalition partners. A U.S. lieutenant colonel explained the situation:

> [A barrier to sharing information] here is the large variety of systems and the lack of interoperability between them.…If I have information that I think needs to be shared, I make sure it gets shared.…But the lack of system integration and disclosure policies do not help very much. CIDNE is a database on SIPR.…It is a good system, but it is a U.S. database on U.S. SIPR. JOIIS is a similar database, but it is a NATO database [on the NATO SECRET network].…Now I have a bunch of guys in my office transferring information between SIPR and NATO SECRET. And when information needs to be transferred from SIPR to NATO SECRET, it has to go through the foreign disclosure officer.

13

[13] Information Sharing in Military Operations ed. Irina Goldenberg Joseph Soeters Waylon H. Dean

Singapore provides a specific capability to our mission…which is a capability that we do not have ourselves. Despite this support, a lot of people are skeptical of network integration.

Singapore is not a NATO nation and Singapore is well known for its intelligence gathering activities. So they may have other motives for being here. The thing is, there is so much information out here and we just want to be sure that this information is dealt with in secure ways. Within NATO, there are agreements on how to deal with information. But with other nations, there aren't. So basically there is no control over the information that is shared with these nations.

14

[14] Information Sharing in Military Operations ed. Irina Goldenberg Joseph Soeters Waylon H. Dean

IT capability. MINUSMA's information sharing IT capability generally proved to be dysfunctional. As one of the respondents in our case study explained:

> Sharing information and reports was impeded because of a very slow satellite connection; it could take up to 15 min to send an email. Also, finding information on the N-disc [a shared drive] or in the shared folders was made more difficult by the low quality data connection.

15

[15] Information Sharing in Military Operations ed. Irina Goldenberg Joseph Soeters Waylon H. Dean