

Team CIRCL
TLP:WHITE

NATO MUG



MISP

Threat Sharing

PLAN FOR THIS SESSION

- Quick introduction of what MISP is
- How can ISACs use MISP?
- Working with unique use-cases

- 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 effort.**

- 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.

SO, WHAT IS MISP NOWADAYS?

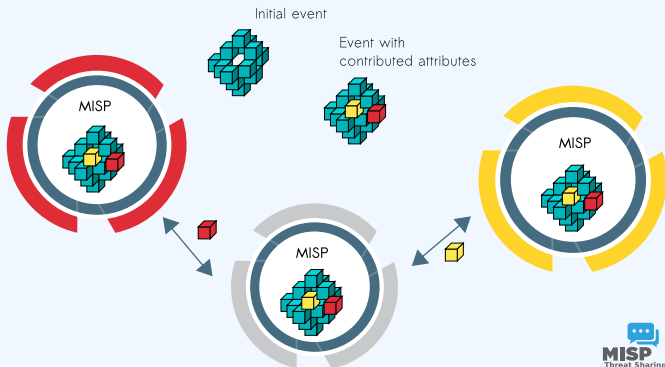
- MISP¹ is a threat information sharing platform that is free & open source.
- MISP has **a host of functionalities** that assist users in creating, collaborating & sharing threat information.
- Long list of connectors to support most of the tooling used by security teams (IDS, Siems, host sensors, analysis tools, etc).
- A rich set of MISP modules² to connect to a wide range of services, easily extended by the users.
- Tools to manage sharing communities and interconnected MISP servers

¹<https://github.com/MISP/MISP>

²<https://www.github.com/MISP/misp-modules>

MISP 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 of entry** to get acquainted with the system.



- Correlating data
- Feedback loop from detections via **Sightings**
- **False positive management** via the warninglist system
- **Enrichment system** via MISP-modules
- **Integrations** with a plethora of tools and formats
- Flexible **API** and support **libraries** such as PyMISP to ease integration
- **Timelines** and giving information a temporal context
- Full chain for **indicator life-cycle management**

WHAT SORT OF SHARING SCENARIOS MAKE SENSE FOR ISACs?

- Exchange of **insights from monitoring**
- Sharing the outcomes of **incidents** (often technical only)
- Information on the **attackers, techniques used**
- **Remediation** information / **prevention** information
- **Vulnerability** pre-disclosure
- Supporting **tools / scripts**

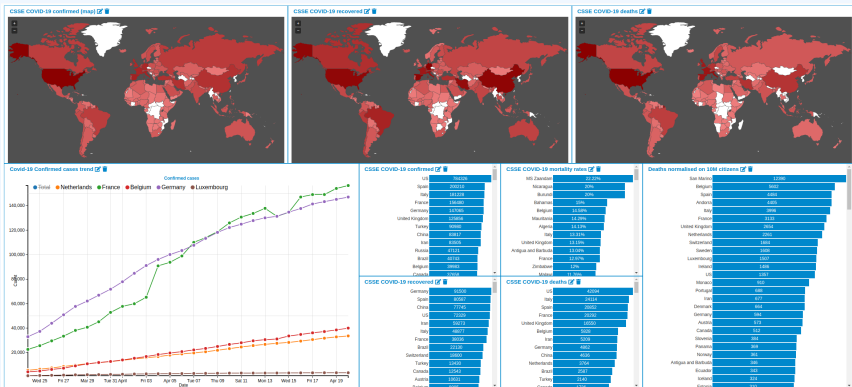
OTHER TYPES OF EXCHANGES WE'VE SEEN (OFTEN BY SECTORIAL ISACS)

- **Financial fraud** information sharing
- Law enforcement / Border control specific sharing
- **Disinformation** sharing
- **Health** related information sharing

AN EXAMPLE OF AN ALTERNATE USE-CASE: COVID-19 MISIP

- COVID-19 MISIP is a MISIP instance retrofitted for COVID-19 info sharing
- We are focusing on three areas of sharing:
 - ▶ **Medical** information
 - ▶ **Cyber threats** related to / abusing COVID-19
 - ▶ **Disinformation** campaigns abusing COVID-19
- Low barrier of entry, aiming for wide spread
- Already a **massive community**

COVID-19 MISP DASHBOARD (MEDICAL DATA PART)



We are rapidly building new models for the different COVID-19 related information sources

SHARING DIFFICULTIES

- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
- Legal restriction³
 - ▶ "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."

³<https://www.misp-project.org/compliance/>

GETTING STARTED WITH COMMUNITIES FOR ISACs

- Different models for constituents
 - ▶ **Connecting to** a MISP central instance hosted by the ISAC
 - ▶ **Hosting** their own instance and connecting to CSIRT's MISP
 - ▶ The ISAC member becoming a "**hub**" for a connected (sub-) community
- Additional services potentially offered
 - ▶ Access to **shared services / subscriptions**
 - ▶ Offering **services** directly through MISP (assisting in incident resolution, etc)
 - ▶ **Collaboration** between members

- ISAC specific **common vocabularies**
- Common tooling / integration options
 - ▶ Already existing, self-built or simply reach out to us for support
- Community management tooling
- **Massive adoption** of MISP means a lot of your members probably already know the tool

WHAT DO MEMBERS OF A COMMUNITY GET OUT OF THIS?

- **Herd immunity** through automatable, actionable protection/detection
- A **collaboration** platform
- Derived metrics and situational awareness to identify gaps / focus areas
- Making **canonisation** and **conversion** of their data sources straight forward for their tooling
- **Near real-time exchange** of automated information

SO WHAT'S THE NEXT STEP FOR A THRIVING COMMUNITY?

- Getting your community to be active takes **time and effort**, but with persistence your chances are great.
- However, most of these communities end up being in a **sectorial/geographic silo**
- The next step is to become part of a network of ISACs, **join broader sharing communities**

ADVANTAGES OF CROSS SECTORIAL SHARING

- **Reuse of TTPs** across sectors
- Being hit by something that **another sector has faced before**
- **Hybrid threats** - how seemingly unrelated things may be interesting to correlate
- Prepare other communities for the capability and **culture of sharing** for when the need arises for them to reach out to CSIRT
- Generally our field is ahead of several other sectors when it comes to information sharing, might as well **spread the love**

■ X-ISAC⁴

- ▶ **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
- ▶ Building an information sharing community and best practices⁵

⁴<https://www.x-isac.org/>

⁵We published the complete guidelines in https://www.x-isac.org/assets/images/guidelines_to_set-up_an_ISAC.pdf

- 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.
- MISP project combines open source software, open standards, best practices and communities to make information sharing a reality.

- 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://gitter.im/MISP/MISP>
<https://twitter.com/MISPProject>



MISP

Threat Sharing

MISP Training Cheat Sheet

Virtual Machine (MISP Training VM)

The MISP Training VM is available at the following location :
<https://www.circl.lu/misp-images/>.

The VM can be imported into VirtualBox or VMWare as an appliance (OVA).

The MISP training VM includes multiple applications and packages which are configured by default without production-ready secure settings. We strongly recommend to not use this VM for production and/or for storing sensitive information.

Default URL and (username/password)

- MISP web interface - <http://127.0.0.1> (NAT: <http://127.0.0.1:8080>) (admin@admin.test/admin)
- MISP-modules - <http://127.0.0.1:6666>
- MISP-dashboard - <http://127.0.0.1:8001>
- Viper-web - <http://127.0.0.1:8888> (admin/Password1234)
- jupyter-notebook - <http://127.0.0.1:8889>
- system credentials via ssh/terminal - (misp/Password1234)

How to get the API key of my user?

Go to the MISP web interface, and simply click your username in the right upper corner to see your user profile which includes your API key.

How to reset a password in MISP?

If you did any specific mistake while setting up your password at the first login. You can reset the password by logging in on the system (via SSH or terminal) and typing the following command:
`/var/www/MISP/app/Console/cake Password admin@admin.test YourTemporaryPassword`

How to reset the bruteforce login protection?

While trying to log into MISP multiple times unsuccessfully, the bruteforce protection might be triggered. You can reset the bruteforce login protection's state by logging into the system (via SSH or terminal) and typing the following command:
`/var/www/MISP/app/Console/cake Admin clearBruteforce`

How to upgrade MISP to the latest version?

Log in via SSH or terminal and type the following commands (your VM must have an Internet access):

1. `cd /var/www/MISP`
2. `git pull origin 2.4`
3. `git submodule update --init --recursive`

Getting OSINT information into your MISP

By default, a fresh installation of MISP is empty as we prefer to leave it up to the users to store, gather, and share the information they need. If you would like to populate your MISP with some real-life data, simply enable the CIRCL OSINT feed, which contains cybersecurity threat-related information. In order to enable the OSINT feed, go to → Sync Actions then → List Feeds. Then select the checkbox next to the first feed (called CIRCL OSINT Feed) and click on top **Enable Selected**. To fetch all events from the selected feed, scroll to the right side of the CIRCL OSINT Feed row and simply click the icon depicting a downward pointing arrow in a circle. Once you go back to the Event Index, the events will start appearing gradually.

Training materials and documentation


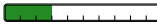
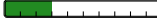
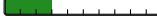


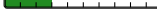
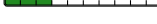
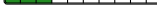


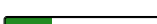
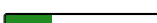

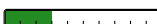
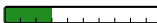
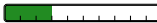
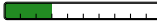
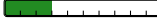
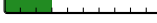
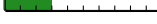
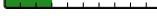
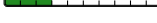
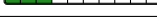

MISP training materials are available at the following location <https://www.circl.lu/services/misp-training-materials/> and are freely licensed under CC-BY-SA. MISP book is available at the following location <https://www.circl.lu/doc/misp/>.

Copyright © 2018 MISP Project licensed under CC-BY-SA

List of features to explain: User (MISP trainer support)

Check	Description	Length
<input type="checkbox"/>	Add events	
<input type="checkbox"/>	- via Standard UI	
<input type="checkbox"/>	- Distribution levels and publication	
<input type="checkbox"/>	- Different type of timestamps	
<input type="checkbox"/>	Add attributes	
<input type="checkbox"/>	- via Freetext	
<input type="checkbox"/>	- via Standard UI	
<input type="checkbox"/>	- via Template	
<input type="checkbox"/>	- via ReST API (including freetext API?)	
<input type="checkbox"/>	- via EventGraph	
<input type="checkbox"/>	Object	
<input type="checkbox"/>	- add Object	
<input type="checkbox"/>	- add References	
<input type="checkbox"/>	- show via EventGraph	
<input type="checkbox"/>	- add additional elements via the EventGraph	
<input type="checkbox"/>	*-lists	
<input type="checkbox"/>	- Warninglists: show warnings raised in steps above	
<input type="checkbox"/>	- Noticelists: show warnings when adding data	
<input type="checkbox"/>	- Import Regexp: avoid leaking private/personal data	
<input type="checkbox"/>	Correlations	
<input type="checkbox"/>	- show correlations that were added	
<input type="checkbox"/>	- pivot to events via correlations	
<input type="checkbox"/>	- show correlations graph	
<input type="checkbox"/>	- feeds & servers correlation	
<input type="checkbox"/>	Tags and Galaxies	
<input type="checkbox"/>	- add Tag from Taxonomy	
<input type="checkbox"/>	- add GalaxyCluster	
<input type="checkbox"/>	- add ATT&CK pattern	
<input type="checkbox"/>	- Creating and using Tag Collection	
<input type="checkbox"/>	Sighting	
<input type="checkbox"/>	- via UI + custom via UI (new source or expiration sighting)	
<input type="checkbox"/>	- via API	
<input type="checkbox"/>	Delegation	
<input type="checkbox"/>	Proposal	
<input type="checkbox"/>	Delete (including soft versus hard delete)	
<input type="checkbox"/>	- Event blacklist when deleting	
<input type="checkbox"/>	Extending event (how and when to use it)	
<input type="checkbox"/>	Extracting the data	
<input type="checkbox"/>	- download from	
<input type="checkbox"/>	- download from via modules	
<input type="checkbox"/>	- .json routing	
<input type="checkbox"/>	- mass export	
<input type="checkbox"/>	- RestSearch	
<input type="checkbox"/>	Searching for data	
<input type="checkbox"/>	- Attribute search	
<input type="checkbox"/>	- Event index filter search	

List of features to explain: Administrator (MISP trainer support)

Check	Description	Length
<input type="checkbox"/>	User	
<input type="checkbox"/>	- administration and contact via standard UI	
<input type="checkbox"/>	- Roles	
<input type="checkbox"/>	Organisations	
<input type="checkbox"/>	- local and remote	
<input type="checkbox"/>	- administration: Creation and merge	
<input type="checkbox"/>	- Org admins and sync users	
<input type="checkbox"/>	Sharing group	
<input type="checkbox"/>	- administration via standard UI	
<input type="checkbox"/>	Templates	
<input type="checkbox"/>	- administration via standard UI	
<input type="checkbox"/>	- Pulling and Updating	
<input type="checkbox"/>	Jobs and Workers	
<input type="checkbox"/>	- administration via standard UI	
<input type="checkbox"/>	- Scheduled Tasks and CRON jobs	
<input type="checkbox"/>	Black listing	
<input type="checkbox"/>	- Events	
<input type="checkbox"/>	- Organisations	
<input type="checkbox"/>	Searching	
<input type="checkbox"/>	- Dashboard	
<input type="checkbox"/>	- Event index	
<input type="checkbox"/>	- Attributes: values, [not] tag	
<input type="checkbox"/>	- Event level: quickfilter, contextual, distribution	
<input type="checkbox"/>	- Event level: event graph	
<input type="checkbox"/>	- RestSearch	

MISP Training Slide Decks

MISP¹ is a threat intelligence platform for gathering, sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information.

This document includes the slides which are the support materials² used for MISP trainings. The content is dual-licensed under CC-BY-SA version 4 license or GNU Affero General Public License version 3 which allows you to freely use, remixes and share-alike the slides while still mentioning the contributors under the same conditions.

Contributors

- Steve Clement <https://github.com/SteveClement>
- Alexandre Dulaunoy <https://github.com/adulau>
- Andras Iklody <https://github.com/iglocska>
- Sami Mokaddem <https://github.com/mokaddem>
- Sascha Rommelfangen <https://github.com/rommelfs>
- Christian Studer <https://github.com/chrisr3d>
- Raphaël Vinot <https://github.com/rafiot>
- Gerard Wagener <https://github.com/haegardev>

Acknowledgment

The MISP project is co-financed and resource supported by CIRCL Computer Incident Response Center Luxembourg³ and co-financed by a CEF (Connecting Europe Facility) funding under CEF-TC-2016-3 - Cyber Security as *Improving MISP as building blocks for next-generation information sharing*.



Co-financed by the Connecting Europe
Facility of the European Union

¹<https://www.misp-project.org/>

²<https://github.com/MISP/misp-training>

³<https://www.circl.lu/>

