

MISP Use Case Report

BoB 8th Kang Seong Min

Contents

- I. What is MISP
- II. Create events
- III. Using API
- IV. MISP-Cloud
- V. Sharing/synchronization
- VI. Use case
- VII. Problems
- VIII. Else

I. What is MISP?

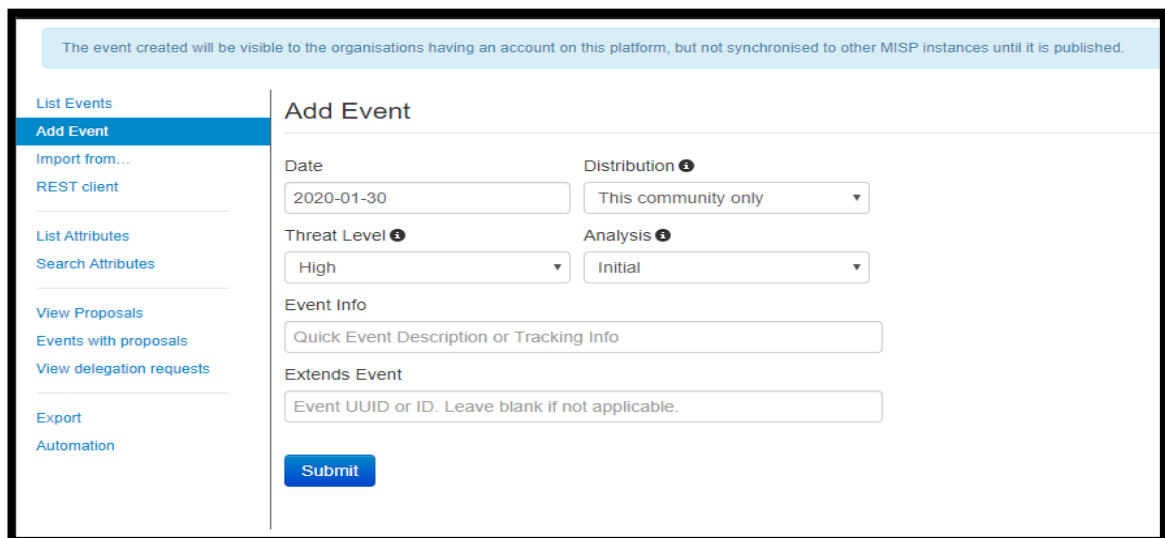
MISP is a threat intelligence platform for sharing, storing and correlating Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information. Discover how MISP is used today in multiple organisations. Not only to store, share, collaborate on cyber security indicators, malware analysis, but also to use the IoCs and information to detect and prevent attacks, frauds or threats against ICT infrastructures, organisations or people.

II. Create events

You can create an event based on a report. I found report about attack could related to North Korea APT Group. I append this information to my MISP Instance. I could add this event by clicking the "Add Event" option or Using API.



figure 1. Report related to North kore apt group



The event created will be visible to the organisations having an account on this platform, but not synchronised to other MISP instances until it is published.

Add Event

Date
2020-01-30

Distribution ⓘ
This community only ▼

Threat Level ⓘ
High ▼

Analysis ⓘ
Initial ▼

Event Info
Quick Event Description or Tracking Info

Extends Event
Event UUID or ID. Leave blank if not applicable.

Submit

Left sidebar menu:
List Events
Add Event
Import from...
REST client
List Attributes
Search Attributes
View Proposals
Events with proposals
View delegation requests
Export
Automation

figure 2. Add Event option


```
C:\Users\SeongMin Kang\Desktop\MISP_API>python create_events.py -h
usage: create_events.py [-h] [-d DISTRIB] [-i INFO] [-a ANALYSIS] [-t THREAT]

Create an event on MISP.

optional arguments:
  -h, --help            show this help message and exit
  -d DISTRIB, --distrib DISTRIB
                        The distribution setting used for the attributes and
                        for the newly created event, if relevant. [0-3].
  -i INFO, --info INFO  Used to populate the event info field if no event ID
                        supplied.
  -a ANALYSIS, --analysis ANALYSIS
                        The analysis level of the newly created event, if
                        applicable. [0-2]
  -t THREAT, --threat THREAT
                        The threat level ID of the newly created event, if
                        applicable. [1-4]
```

figure 3. Create events by using API

Using these option, I could add Date, Distribution(choose sharing range), Threat Level, Analysis, Event Info. Additionally could make tags by using "Add tag" or API. By using tags, we could know the events is related to what efficiently.



The screenshot shows the 'Add Tag' form in the MISP web interface. On the left is a sidebar with links: 'List Favourite Tags', 'List Tags', and 'Add Tag' (which is highlighted). The main form area is titled 'Add Tag' and contains the following fields and controls:

- Name:** A text input field.
- Colour:** A text input field.
- Restrict tagging to org:** A dropdown menu currently set to 'Unrestricted'.
- Restrict tagging to user:** A dropdown menu currently set to 'Unrestricted'.
- Exportable:** A checked checkbox.
- Hide Tag:** An unchecked checkbox.
- Add:** A blue button to submit the form.

figure 4. Add Tag options

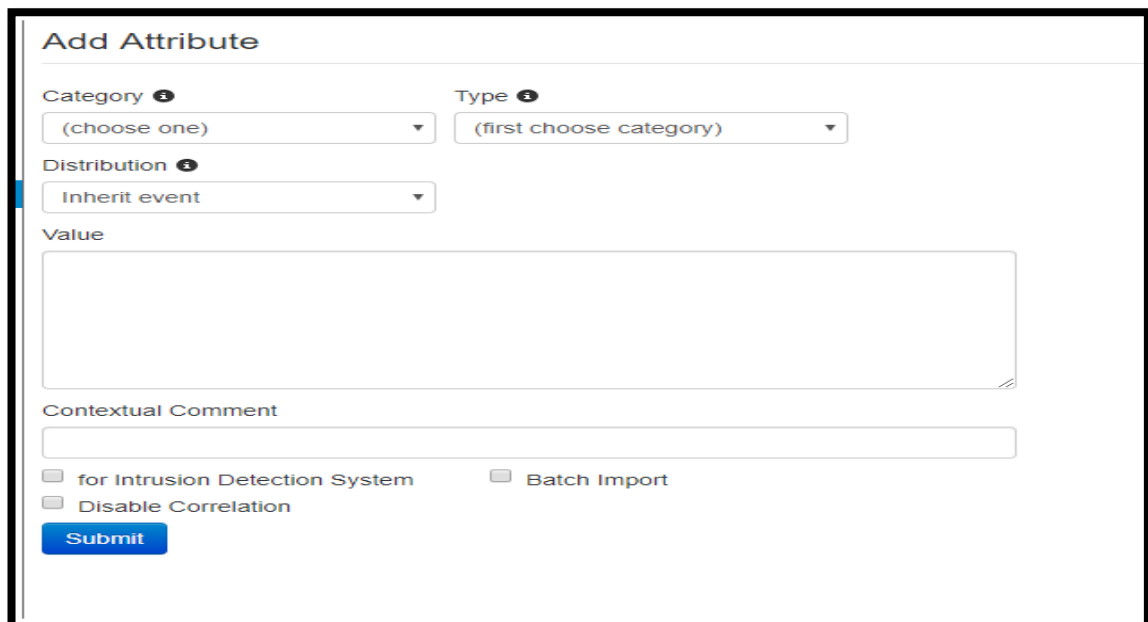
```
C:\WP\MISP-master\WP\MISP-master\examples>python addtag.py -h
usage: addtag.py [-h] -e EVENT [-a ATTRIBUTE] -t TAG [-m]

Get an event from a MISP instance.

optional arguments:
  -h, --help            show this help message and exit
  -e EVENT, --event EVENT
                        Event ID to get.
  -a ATTRIBUTE, --attribute ATTRIBUTE
                        Attribute ID to modify. A little dirty for now,
                        argument need to be included in event
                        Tag ID.
  -t TAG, --tag TAG      Tag ID.
  -m, --modify_attribute
                        If set, the tag will be add to the attribute,
                        otherwise to the event.
```

figure 5. Add Tag by using API

And we could add attributes(loC, reports link...etc) to events by using "Add Attribute" or API.
Or could append using Free text tool by clicking



The screenshot shows the 'Add Attribute' form in the MISP web interface. The form contains the following fields and controls:

- Category:** A dropdown menu with '(choose one)' selected.
- Type:** A dropdown menu with '(first choose category)' selected.
- Distribution:** A dropdown menu with 'Inherit event' selected.
- Value:** A large text area for entering the attribute value.
- Contextual Comment:** A text input field.
- for Intrusion Detection System:** An unchecked checkbox.
- Disable Correlation:** An unchecked checkbox.
- Batch Import:** An unchecked checkbox.
- Submit:** A blue button to submit the form.

figure 6. Add Attribute options

```
C:\Users\SeongMin Kang\Desktop\MISP_API>python add_named_attribute.py -h
usage: add_named_attribute.py [-h] [-e EVENT] [-t TYPE] [-v VALUE]

Add an attribute to an event

optional arguments:
  -h, --help            show this help message and exit
  -e EVENT, --event EVENT
                        The id, uuid or json of the event to update.
  -t TYPE, --type TYPE  The type of the added attribute
  -v VALUE, --value VALUE
                        The value of the attribute
```

figure 7. Add Attribute by using API

You also could add attribute by using Freetxt Import tool. It allings attributes about their characteristics.



figure 8. Free text tool button

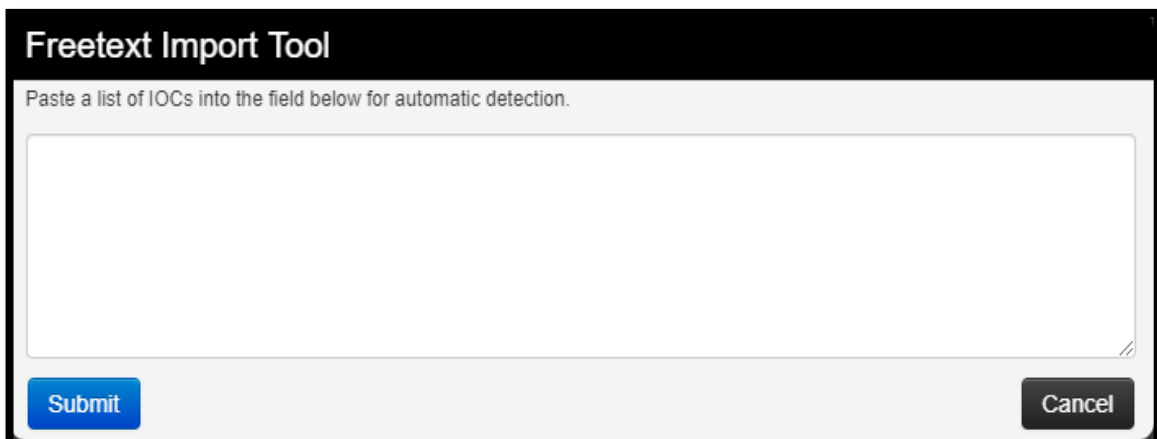
A screenshot of the 'Freetext Import Tool' interface. The title bar at the top reads 'Freetext Import Tool'. Below the title bar, there is a text area with the instruction 'Paste a list of IOCs into the field below for automatic detection.' The text area is empty. At the bottom of the interface, there are two buttons: a blue 'Submit' button on the left and a grey 'Cancel' button on the right.

figure 9. Freextext Import Tool

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Actions
2020-01-29		Artifacts dropped	sha1	8a5f25624745e5cf1e47da8cfb009795990f367				<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	md5	#8e6941d28e5b2b271141eeb7f1fc07				<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	sha1	adb77911889c017a6cb7ef6fa#6214e2a7e9926				<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	sha1	d9f1029681f805f09784517348d04f49146dbde8				<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	(0/0/0)	
2020-01-29		Network activity	url	http://kjinnong.com/jdboard/boardbank/board/bbs/log.php				<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	sha256	36eb516468600b1149f039e4a95560958ae9e23292687c031fe8150e8e8e0d				<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	sha256	68200e459cfd503c118b848777acel7c9cbfc0b2d0b69b5d5b98e767cd63849				<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	sha256	c272f89776518db4a156bc5c683bc4ed3b089c88ec59a99cecae0654fda808				<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	md5	1678bd99d0433d42f7643cf167bc267b				<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	md5	98ed4f9eb07f0a6c4f2f40fa539016d				<input checked="" type="checkbox"/>			<input checked="" type="checkbox"/>	Inherit	(0/0/0)	
2020-01-29		External analysis	link	http://blog.alysac.co.kr/1527				<input checked="" type="checkbox"/>			<input type="checkbox"/>	All	(0/0/0)	

figure 10. Attributes added by Freetext import tool

III. Using API

PyMISP is a Python library to access MISP platforms via their REST API. You can Install PyMISP by either pip or by getting the last version from the Github repository¹. Before using this, you should know your baseurl and Auth key. You can find your Auth key in <https://<baseurl>/users/view/me>.

User	
Id	1
Email	admin@admin.test
Organisation	First
Role	admin
Autoalert	No
Authkey	93RiITeyNXmvTKYgscaLEG5AGYZkRhVqLhQTYUY1 (reset)
Terms accepted	No
GnuPG key	N/A

figure 11. Auth key

I made API with regex and using Curl.

¹ <https://github.com/MISP/PyMISP>

```
def check_data_character(data):
    md5 = re.findall(r"([a-fA-F\d]{32})", data)
    sha1 = re.findall(r"([a-fA-F\d]{40})", data)
    sha256 = re.findall(r"([a-fA-F\d]{64})", data)
    IP = re.findall(r"(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)", data)
    Email = re.findall(r"([a-z]([_a-z0-9-]+@[a-z0-9-]+\.[a-z]+)\b)", data)
    CVE = re.findall(r"([a-z]{4}\-[0-9]{4}\-[0-9]{4,6})\b)", data)
    Filename = re.findall(r"([A-Za-z0-9_\.]+\.(exe|dll|bat|sys|htm|html|js|jar|jpg|png|vb|scr|pif|chm|zip|rar|cab|pdf|doc|docx|ppt|pptx|xls|xlsx|swf|gif))\b)", data)
```

Figure 12. regex to find IoCs

The command about curl could be found in MISP API document². Using this code. I uploaded bulk of locs to my MISP instance.

✓	5	APT 37	169	1	gangseongmin18@gmail.com	2020-01-31	APT 37
✓	6	Kimsuki	94	1	gangseongmin18@gmail.com	2020-01-31	Kimsuki

Figure 13. uploaded locs

Also you could add tags to events or each of IoCs. Tag is important for distinguish the Attacker group. You can check this option in "Event Actions"

91	✓	✗	APT
94	✓	✗	APT 37
3	✓	✗	Andariel

Figure 14. Tags

If there exist same IoCs with other events, MISP create Correlation Graph

² <https://www.circl.lu/doc/misp/automation/>

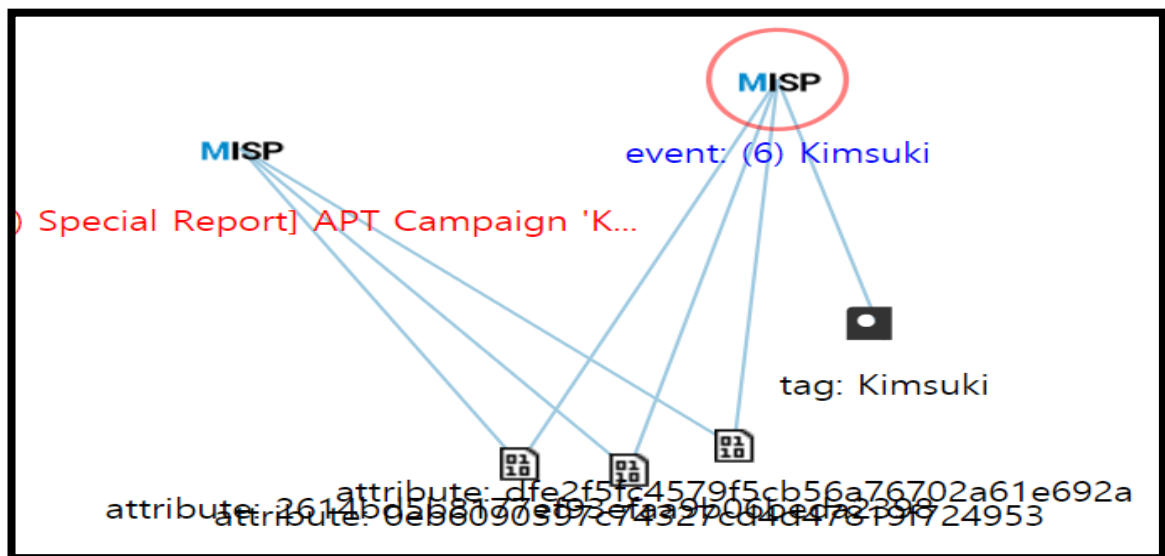


Figure 15. Correlation Graph

IV. MISP-Cloud

You can install MISP in EC2 instance by selecting MISP-Cloud

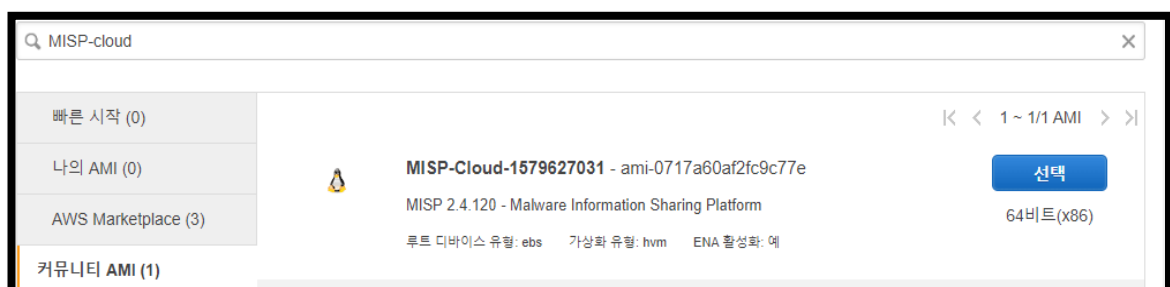


figure 12. MISP-Cloud

Start by selecting "**Community AMIs**" and search for **MISP-Cloud**. The builds are always created with "MISP" and the creation date. Chose "Select" after finding the MISP image.

단계 2: 인스턴스 유형 선택

Amazon EC2는 각 사용 사례에 맞게 최적화된 다양한 인스턴스 유형을 제공합니다. 인스턴스는 애플리케이션을 실행할 수 있는 가상 서버입니다. 이러한 인스턴스에는 CPU, 메모리, 스토리지 및 네트워킹 용량의 다양한 조합이 있으며, 애플리케이션에 사용할 적절한 리소스 조합을 유연하게 선택할 수 있습니다. 인스턴스 유형과 이 인스턴스 유형이 컴퓨팅 요건을 충족하는 방식에 대해 [자세히 알아보기](#).

필터링 기준: 모든 인스턴스 유형 현재 세대 열 표시/숨기기

현재 선택된 항목: t2.micro (Variable ECU, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB 메모리, EBS 전용)

	그룹	유형	vCPUs	메모리 (GiB)	인스턴스 스토리지 (GB)	EBS 최적화 사용 가능	네트워크 성능	IPv6 지원
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS 전용	-	낮음에서 중간	예
<input checked="" type="checkbox"/>	General purpose	t2.micro 프리 티어 사용 가능	1	1	EBS 전용	-	낮음에서 중간	예
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS 전용	-	낮음에서 중간	예
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS 전용	-	낮음에서 중간	예
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS 전용	-	낮음에서 중간	예

figure 13. Choose instance type

The images are built to run on a t2.micro instance, which falls under the "Free Tier" option of AWS. You're free to select another instance type. You can accept the defaults and proceed until **Step 6** where you'll get to configure the firewall rules (*security groups*):

단계 6: 보안 그룹 구성

보안 그룹은 인스턴스에 대한 트래픽을 제어하는 방화벽 규칙 세트입니다. 이 페이지에서는 특정 트래픽을 인스턴스에 도달하도록 허용할 규칙을 추가할 수 있습니다. 예를 들면 웹 서버를 설정하여 인터넷 트래픽을 인스턴스에 도달하도록 허용하려는 경우 HTTP 및 HTTPS 트래픽에 대한 무제한 액세스를 허용하는 규칙을 추가합니다. 새 보안 그룹을 생성하거나 아래에 나와 있는 기존 보안 그룹 중에서 선택할 수 있습니다. Amazon EC2 보안 그룹에 대해 [자세히 알아보기](#).

보안 그룹 할당: ☒ 새 보안 그룹 생성 ☐ 기존 보안 그룹 선택

보안 그룹 이름:

설명:

유형	프로토콜	포트 범위	소스	설명
SSH	TCP	22	위치 무관 0.0.0.0/0, ::/0	예: SSH for Admin Desktop
HTTPS	TCP	443	위치 무관 0.0.0.0/0, ::/0	예: SSH for Admin Desktop

figure 14. Security settings

MISP-Cloud requires at least 443 (*HTTPS*). You can always choose **My IP** to restrict the source to your IP address. After that, you'll be able to launch your instance. Before doing that, however, you need to handle SSH access (*even if you don't plan on using it, AWS requires this step to be completed*):

V. Sharing/synchronization

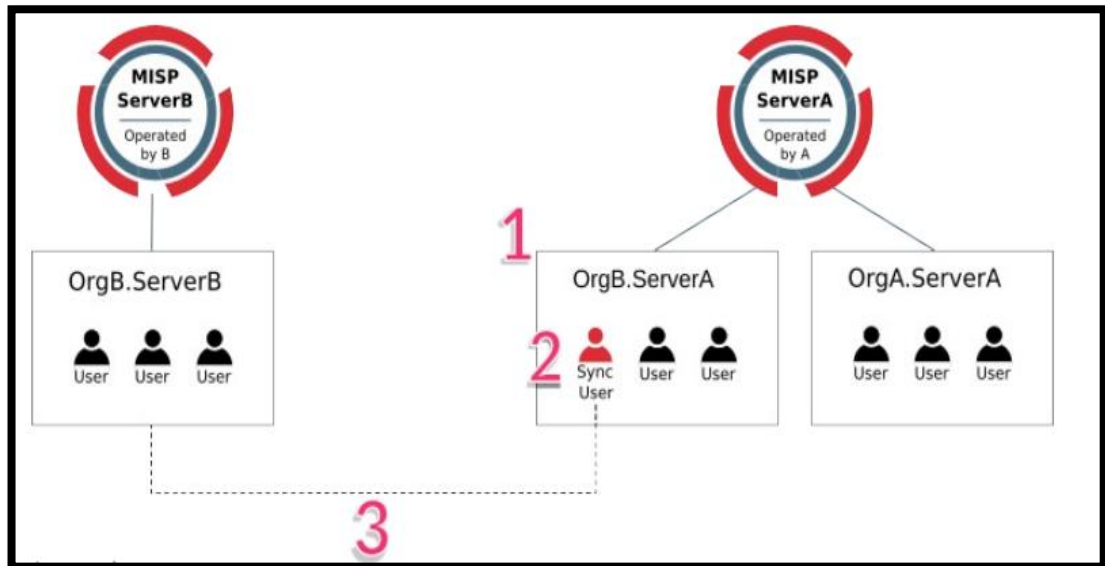


figure 15. Synchronization diagram

Step 1: Add OrgB as a local organisation on ServerA (OrgB.ServerA) using OrgB's existing UUID from their local organisation on ServerB.

Step 2: Add a Sync User (syncuser@OrgB.ServerA) in the organisation OrgB.ServerA on the MISP ServerA.

Step 3: Set up a sync server on MISP ServerB using the key (called Authkey) from the sync user (syncuser@OrgB.ServerA) created on MISP ServerA.

Step 1:

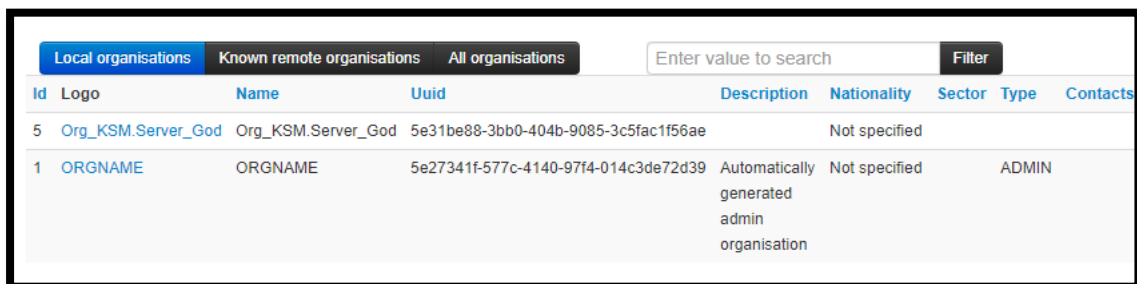
I try this server B(<https://3.87.219.193>), server A(52.90.175.205)

I append Org_KSM.Server_KSM to server B

Local organisations		Known remote organisations		All organisations		Enter value to search		Filter
Id	Logo	Name	Uuid	Description	Nationality	Sector	Type	
1	First	First	5de95b6c-da34-475e-9a6d-343d235e93a4	Automatically generated admin organisation	Not specified		A	
5	Org_KSM.Server_KSM	Org_KSM.Server_KSM	5e31be88-3bb0-404b-9085-3c5fac1f56ae		Not specified			

figure 16. Add orgB.ServerB

And append this organization to server A as local organization

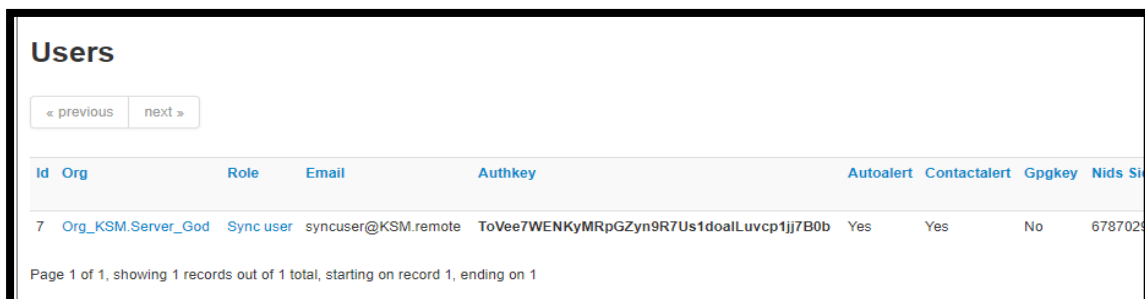


Id	Logo	Name	Uuid	Description	Nationality	Sector	Type	Contacts
5	Org_KSM.Server_God	Org_KSM.Server_God	5e31be88-3bb0-404b-9085-3c5fac1f56ae		Not specified			
1	ORNAME	ORNAME	5e27341f-577c-4140-97f4-014c3de72d39	Automatically generated admin organisation	Not specified		ADMIN	

figure 17. Add OrgB.Server A

Step 2:

I Add sync user in Org_KSM.Server_God organization

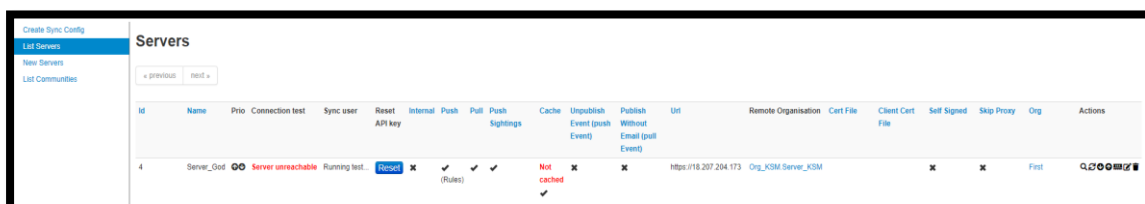


Id	Org	Role	Email	Authkey	Autoalert	Contactalert	Gpgkey	Nids	Sigs
7	Org_KSM.Server_God	Sync user	syncuser@KSM.remote	ToVee7WENkyMRpGZyn9R7Us1doalLuvcp1jj7B0b	Yes	Yes	No	6787029	

figure 18: Add sync user in OrgB.Server A

Step 3:

Add Server by using "New Servers" option(Sync Actions -> List Servers -> New Servers) I fill Auth key with Sync user in Org_KSM.Server_GOd



Id	Name	Prio	Connection test	Sync user	Reset API key	Internal	Push	Pull	Push Signings	Cache	Unpublish Event (push Event)	Publish Without Email (pull Event)	URI	Remote Organisation	Cert File	Client Cert File	Self Signed	Skip Proxy	Org	Actions
4	Server_God	00	Server unreachable	Running test...	Reset	✓	✓	✓	✓	Not cached	✗	✗	https://18.207.204.173	Org_KSM.Server_KSM			✗	✗	First	

figure 19. Add Server by fill auth key with sync users' auth key

VI. Use case

I made two events related to apt 37, Kimsuki. Two groups are related to North Korea. I uploaded total 267 IoCs using automate API. MISP show correlation IoC in events. For Example, I uploaded ioc related to the report about "Continued targeting of cryptocurrencies in South Korea". I could find 6 attribute was related. By using this graph. We

VII. Problems

1. Redirect strange IP

It direct strange IP sometimes. My MISP instance ip is 3.87.219.193 but, sometimes the site go to 3.87.222.81. I solved the problem by changing contents of "/var/www/MISP/app/Config/config.php" file. The base url was set 3.87.222.81, I changed it to 3.87.219.193. The problem solved.

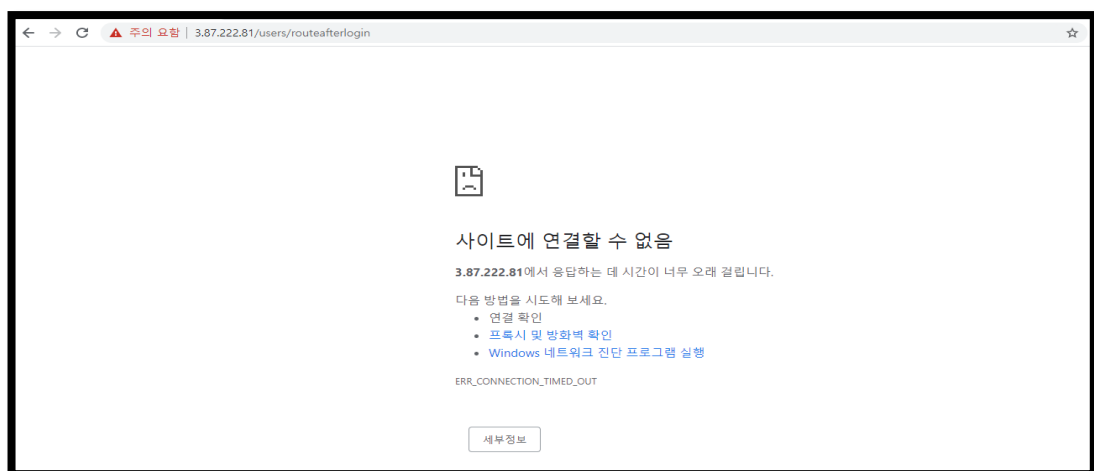


figure 20. Problems with redirecting wrong ip address

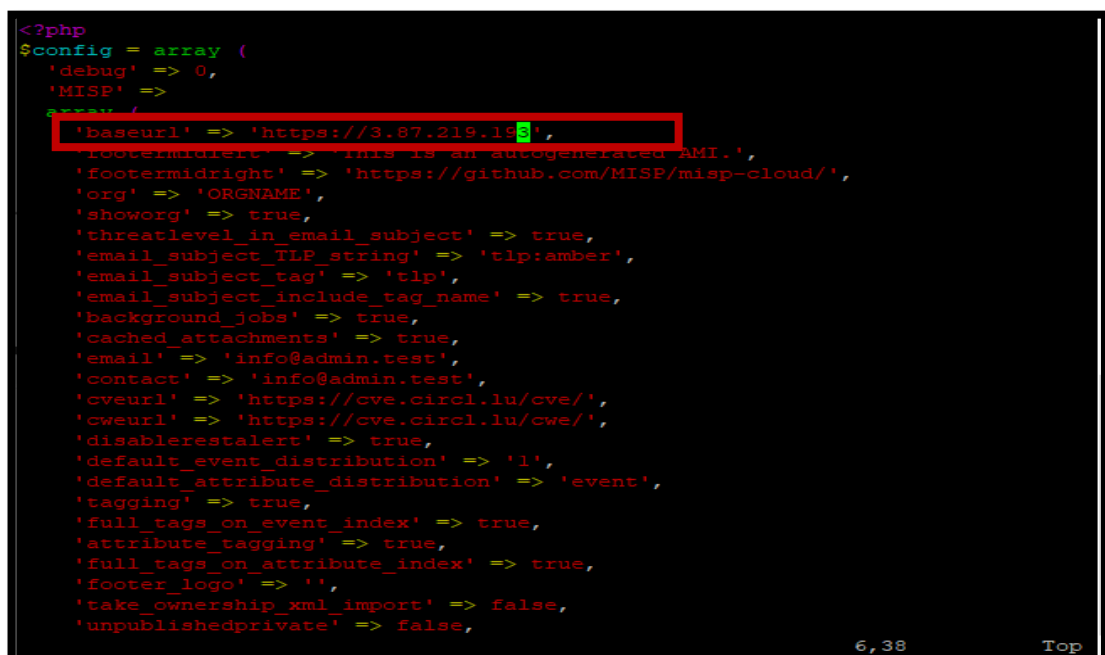


figure 21. Checking base url

2. Synchronizing Errors(server unreachable)

I try to synchronize with another MISP instance by following step of MISP user guide. But failed. Server unreachable error occurred. SSL certification error occurred. To solve this problem, It is important to check "self Signed" box. I solved connection problem and check the Other student's instance.

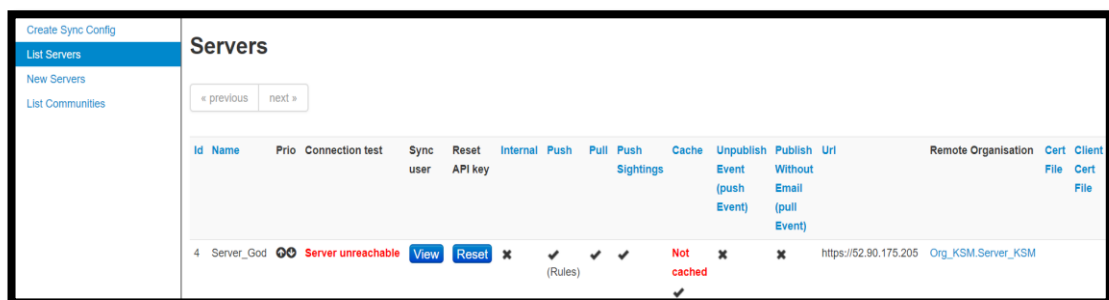


Figure 22. Server unreachable error

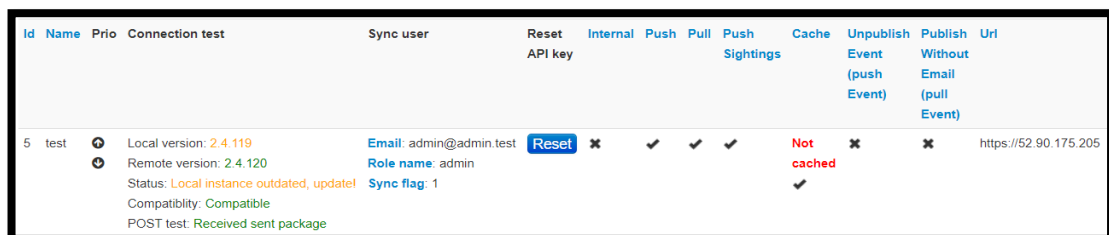


Figure 23. Check Server Connection

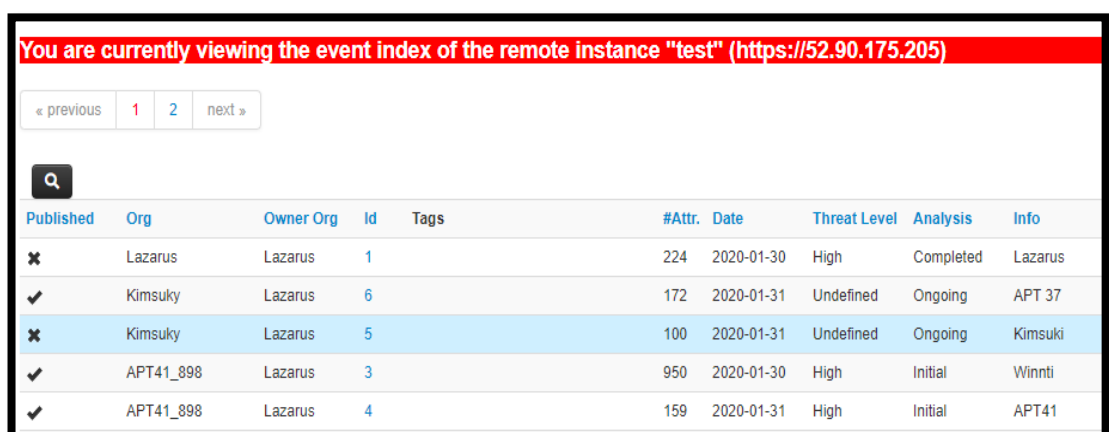


Figure 24. Check Other instance's Events

You can add Other instance's events to Sharing Group in Global actions -> Add Sharing Group

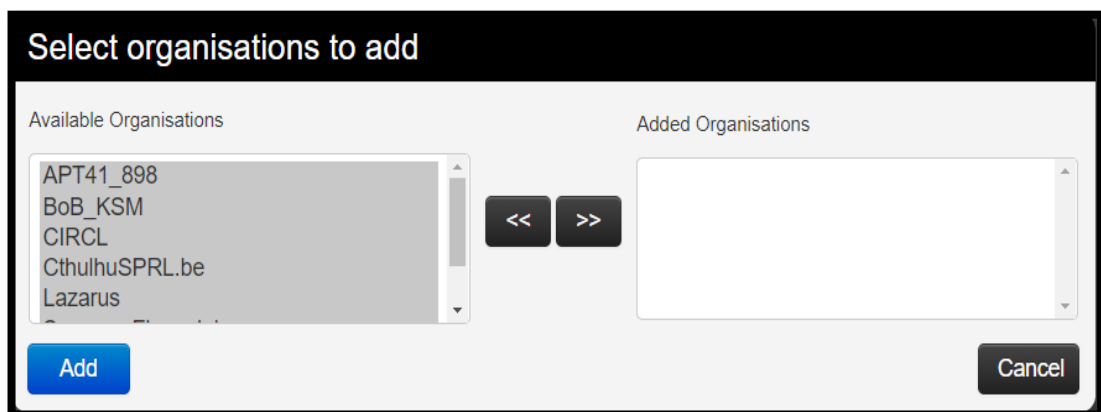


Figure 25. Select Sharing groups

3. API misp_verificert error

To use PyMISP, should set information of url, Authkey, verificert. First, I set the verifier "True" because it related to security problems, and user guide set "ture" but the error occurred. I solve this problem by change setting "True" to "False."

```
[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: self signed certificate (_ssl.c:1076)'))
```

Figure 26. PyMISP SSL Certificate error

```
keys.py > ...
1  misp_url = "https://3.87.219.193/"
2  misp_key = '93RltTeyNXmvTKYgscaLEG5AGYZkRhVqLhQTYUY1'
3  misp_verifycert = False
```

Figure 27. Change verifycert option to "False"

VIII. Else

1. Feed

Feeds are remote or local resources containing indications that can be automatically imported in MISP at regular intervals. You can check or add Feeds in "Sync Actions -> Feeds".

Feeds

Generate feed lookup caches or fetch feed data (enabled feeds only)

Cache all feeds Cache freetext/CSV feeds Cache MISP feeds **Fetch and store all feed data**

« previous 1 2 next »

Default feeds Custom feeds **All feeds** Enabled feeds

<input type="checkbox"/>	Id	Enabled	Caching enabled	Name	Feed Format	Provider
<input type="checkbox"/>	1	✗	✗	CIRCL OSINT Feed MISP	MISP Feed	CIRCL
<input type="checkbox"/>	2	✗	✗	The Botvrij.eu Data MISP	MISP Feed	Botvrij.eu
<input type="checkbox"/>	3	✗	✗	blockrules of rules.emergingthreats.net MISP	Simple CSV Parsed Feed	rules.emergingthreats.net

Figure 28. Feeds

2. MISP Communities

MISP is an open source software and it is also a large community of MISP users creating, maintaining and operating communities of users or organizations sharing information about threats or cyber security indicators worldwide. The MISP project doesn't maintain an exhaustive list of all communities relying on MISP especially that some communities use MISP internally or privately.



circl.lu
Computer Incident
Response Center
LUXEMBOURG

**Community CIRCL Private Sector Information Sharing
Community - aka MISPPRIV**

Figure 29. Misp community