

MISP Use Case Report

BoB 8th Kang Seong Min

Contents

- I. What is MISP
- II. Create events – andariel
- III. Using API
- IV. MISP-Cloud
- V. Sharing/synchronization
- VI. Problems

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 - andariel

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

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' interface. On the left is a sidebar with links: 'List Favourite Tags', 'List Tags', and 'Add Tag' (which is highlighted). The main 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 showing 'Unrestricted'.
- Restrict tagging to user:** A dropdown menu currently showing 'Unrestricted'.
- Exportable:** A checked checkbox.
- Hide Tag:** An unchecked checkbox.
- Add:** A blue button at the bottom left.

figure 4. Add Tag options

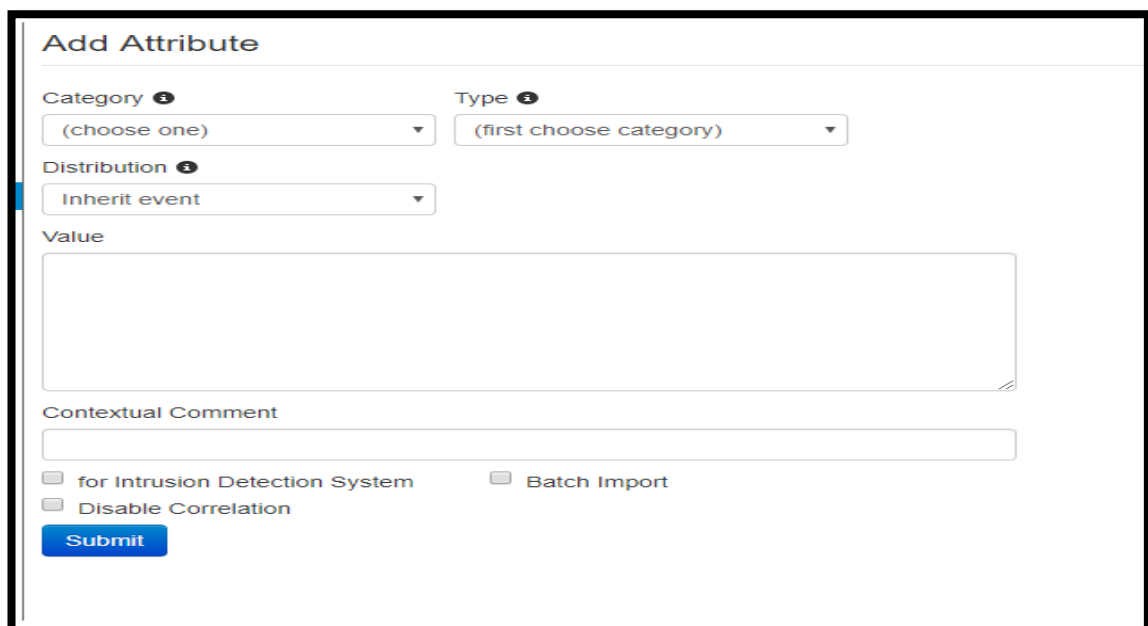
```
C:\WPyMISP-master\WPyMISP-master\examples>python addtag.py -h
usage: addtag.py [-h] -e EVENT [-a ATTRIBUTE] -t TAG [-m]

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' interface. It 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 at the bottom left.

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

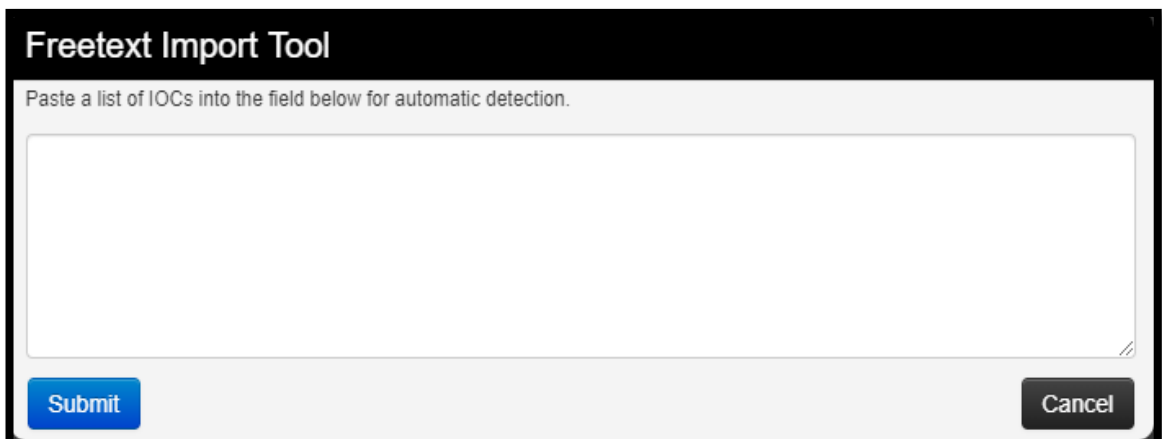
A screenshot of the 'Freetext Import Tool' interface. The title bar says 'Freetext Import Tool'. Below the title bar, there is a text input field with the placeholder text 'Paste a list of IOCs into the field below for automatic detection.' At the bottom of the interface, there are two buttons: a blue '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	Act
2020-01-29		Artifacts dropped	sha1	8a5f25624745e5cf1e47da8cfb009795990f367	+	+		✓			✓	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	md5	#8e6941d28e5b2b271141eeb7f1fc07	+	+		✓			✓	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	sha1	adb77911889c017a6cb7ef6fa#6214e2a7e9926	+	+		✓			✓	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	sha1	d9f1029681f805f09784517348d04f49146dbde8	+	+		✓			✓	Inherit	(0/0/0)	
2020-01-29		Network activity	url	http://kjinnong.com/jdboard/boardbank/board/bbs/log.php	+	+		✓			✓	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	sha256	36eb516468600b1149f039e4a95560958ae9e23292687c031fe8150e8e8e0d	+	+		✓			✓	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	sha256	68200e459cfd503c118b848777acel7c9cbfc0b2d0b69b5d5b98e767cd63849	+	+		✓			✓	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	sha256	c272f89776518db4a156bc5c683bc4ed3b089c88ec59a99cecae0654fda308	+	+		✓			✓	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	md5	1678bd99d0433d42f7643cf167bc267b	+	+		✓			✓	Inherit	(0/0/0)	
2020-01-29		Artifacts dropped	md5	98ed4f9eb07f0a6c4f2f40fa539016d	+	+		✓			✓	Inherit	(0/0/0)	
2020-01-29		External analysis	link	http://blog.alysac.co.kr/1527	+	+		✓				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

¹ <https://github.com/MISP/PyMISP>

IV.MISP-Cloud

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

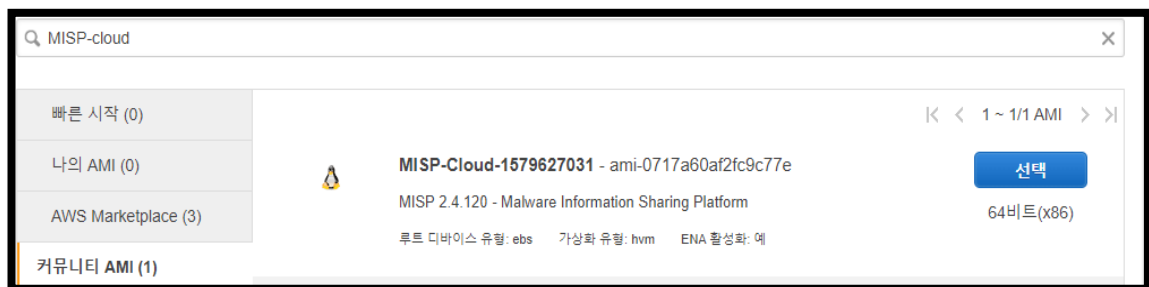


figure 12. MISP-Cloud

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.



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

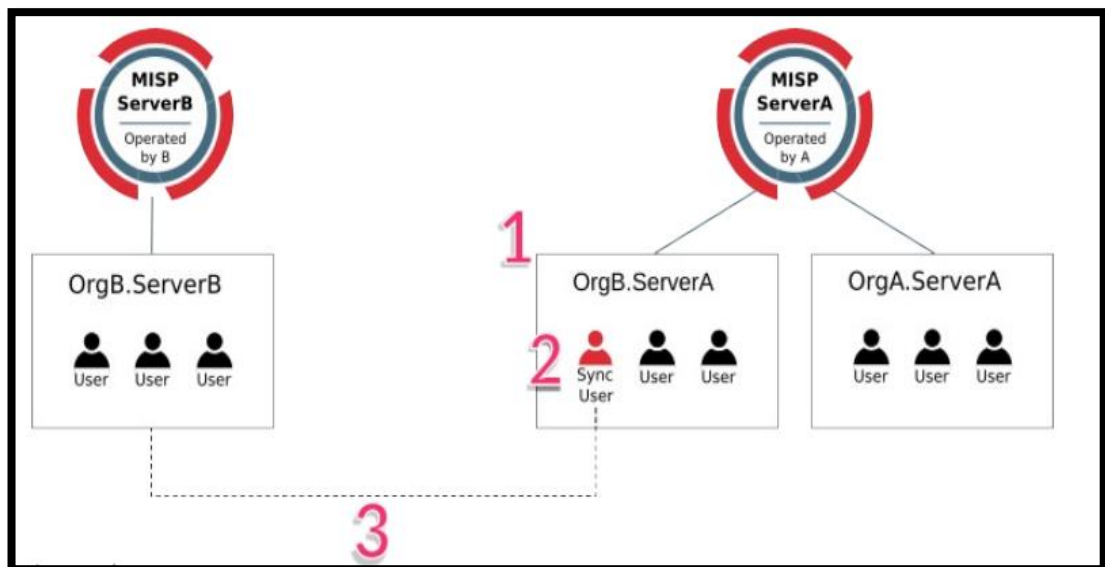


figure 15. Synchronization diagram

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

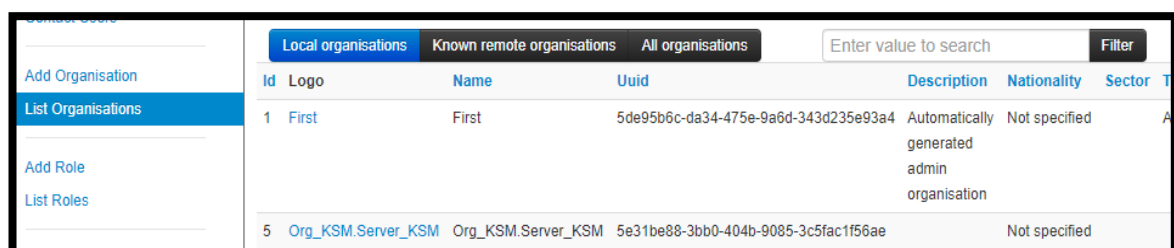
MISP ServerA.

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)

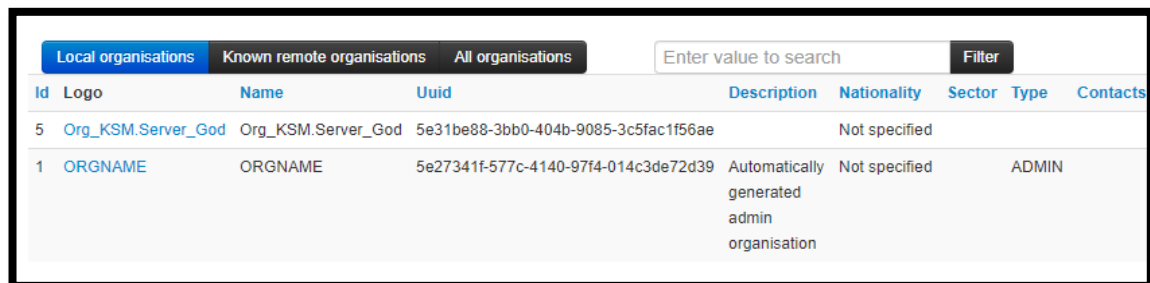
I append Org_KSM.Server_KSM to server B



Organisations							
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		
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

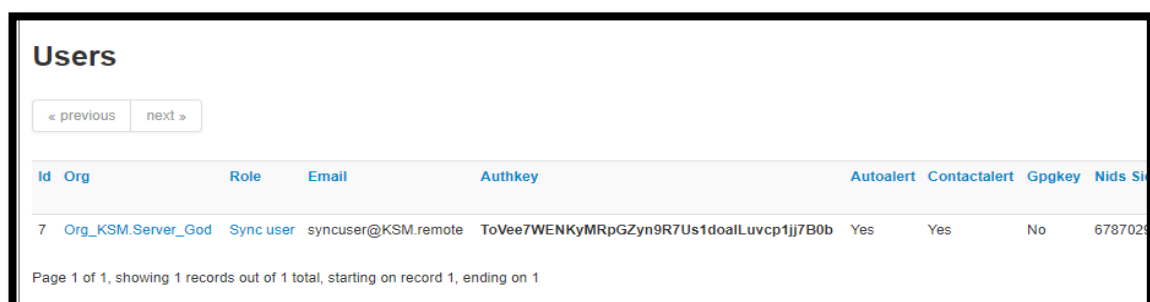


Organisations							
Local organisations Known remote organisations All organisations							
Enter value to search Filter							
Id	Logo	Name	Uuid	Description	Nationality	Sector	Type
5	Org_KSM.Server_God	Org_KSM.Server_God	5e31be88-3bb0-404b-9085-3c5fac1f56ae		Not specified		
1	ORGNAME	ORGNAME	5e27341f-577c-4140-97f4-014c3de72d39	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



Users									
« previous next »									
Id	Org	Role	Email	Authkey	Autoalert	Contactalert	Gpgkey	Nids Sk	
7	Org_KSM.Server_God	Sync user	syncuser@KSM.remote	ToVee7WENKyMRpGZyn9R7Us1doalLuvcp1jj7B0b	Yes	Yes	No	6787029	

Page 1 of 1, showing 1 records out of 1 total, starting on record 1, ending on 1

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	Priv	Connection test	Sync user	Reset API key	Internal	Push	Pull	Sightings	Cache	Unpublish Event (push)	Publish Without Email (pull Event)	URL	Remote Organisation	Cert File	Client Cert File	Self Signed	Skip Proxy	Org	Actions
4	Server_GoD	GO	Server unreachable	Running test...	Reset	X	✓	✓	✓	Not cached	X	X	https://192.207.204.173	Org_KSM.Server_KSM	X	X	X	X	First	

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

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.

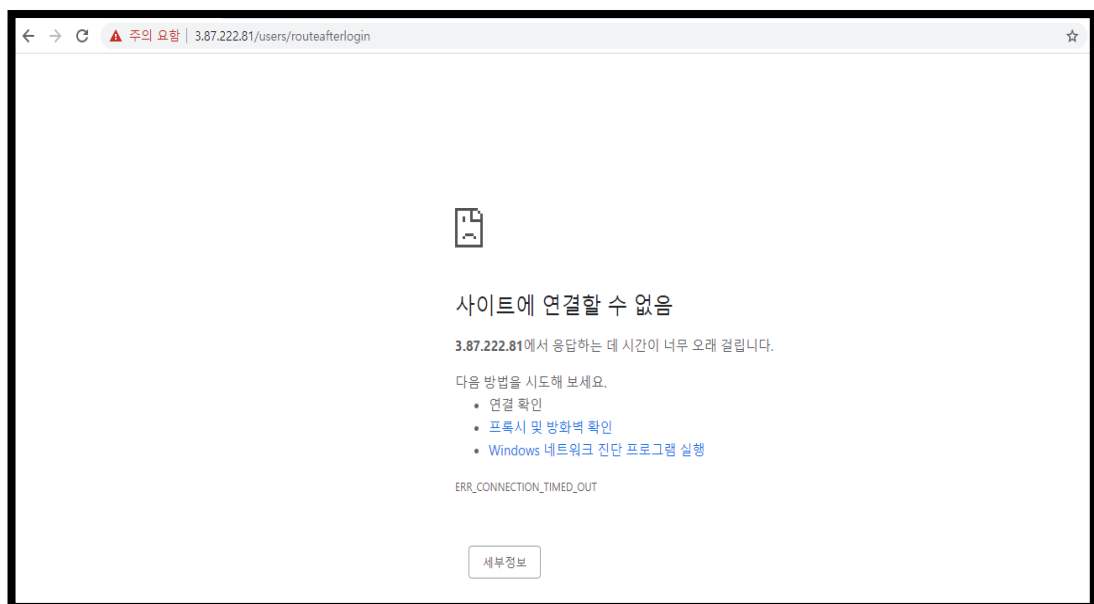


figure 20. Problems with redirecting wrong ip address

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.

Create Sync Config

List Servers

New Servers

List Communities

Servers

« previous

next »

Id	Name	Prio	Connection test	Sync user	Reset API key	Internal	Push	Pull	Push Sightings	Cache	Unpublish Event (push Event)	Publish Without Email (pull Event)	Url	Remote Organisation	Cert File	Client Cert File
4	Server_God	🔴	Server unreachable	View	Reset	✖	✔	✔	✔	Not cached	✖	✖	https://52.90.175.205	Org_KSM.Server_KSM		
<div>(Rules)</div>																