botconf
The botnet fighting conference 2018
sixième édition
6
TOULOUSE
Ateliers le 4 décembre 2018
Conférences du 5 au 7 décembre 2018

Detect, Investigate & Respond Using MISP, TheHive & Cortex

Workshop

Tue Dec 4, 2018

Danni Co, Raphaël Vinot & Saâd Kadhi

Dear Workshop Attendees,

During our journey together, we will cover the following topics:

- Quick overview of the software stack: TheHive, Cortex & MISP
- Installation & Configuration
- Case Study 1: Your Car is Waiting
- Case Study 2: Feed me an Alert
- Case Study 3: Knock, Knock, you've got an Event

For the duration of the workshop, we will give you access to:

- A Cortex server configured with several subscription-based and commercial analyzers.
- A MISP instance that contains several hundreds of events.

Warning

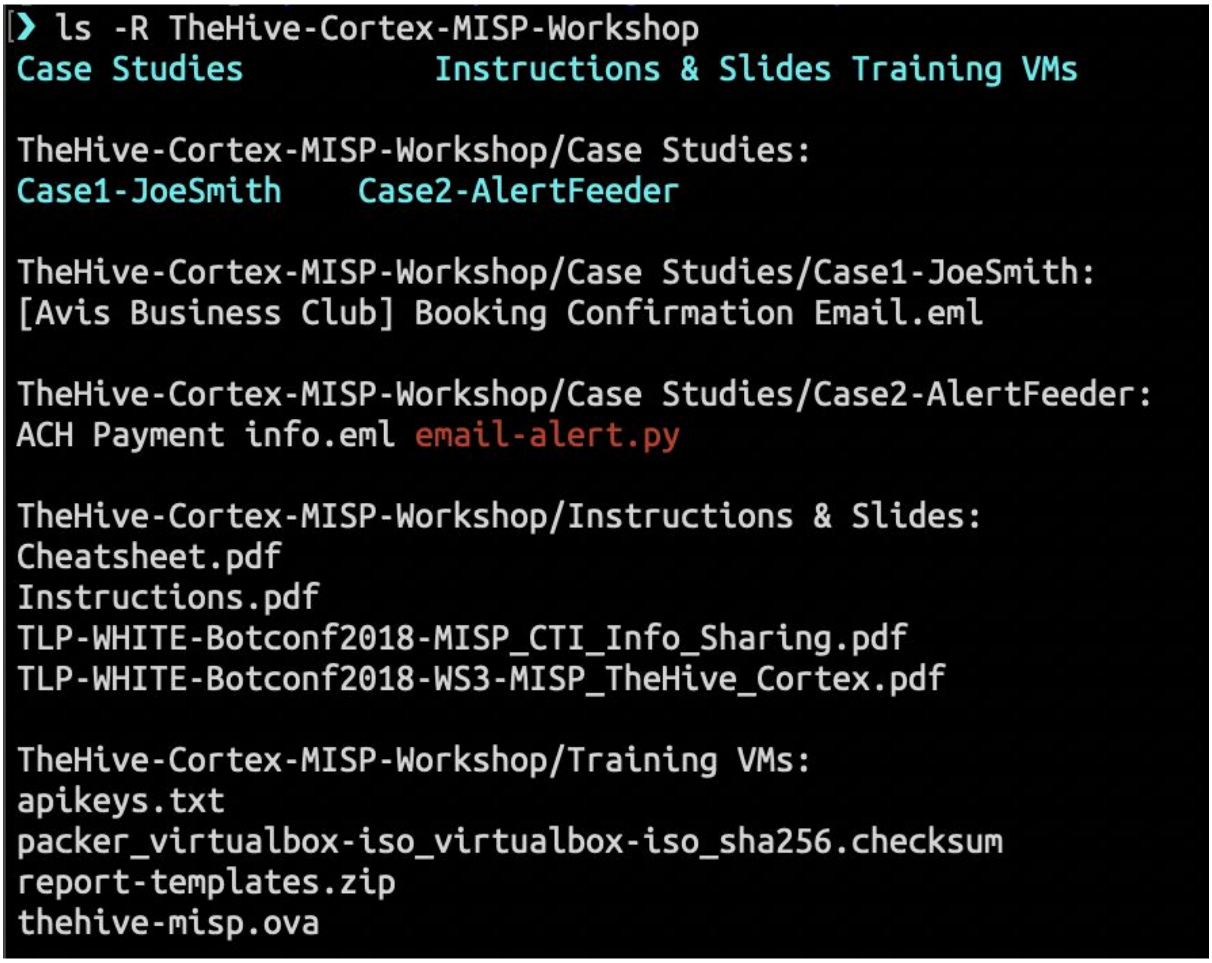
The case studies require manipulating malicious files. **You must use extra caution when manipulating them**. You can upload password-protected ZIP files directly to TheHive without having to decrypt them beforehand.

The instructors cannot be held liable in any way if you accidentally infect your computer. If you don't agree with these terms, do not copy the contents of the workshop USB keys to your computer.

Table of Contents

Copy the Files

The files you will need for the workshop are on the USB keys distributed by the instructors. Once you get a USB key, please copy all the contents to your laptop and pass it on to another attendee or hand it back to the instructors.



```
❯ ls -R TheHive-Cortex-MISP-Workshop
Case Studies           Instructions & Slides Training VMs

TheHive-Cortex-MISP-Workshop/Case Studies:
Case1-JoeSmith    Case2-AlertFeeder

TheHive-Cortex-MISP-Workshop/Case Studies/Case1-JoeSmith:
[Avis Business Club] Booking Confirmation Email.eml

TheHive-Cortex-MISP-Workshop/Case Studies/Case2-AlertFeeder:
ACH Payment info.eml email-alert.py

TheHive-Cortex-MISP-Workshop/Instructions & Slides:
Cheatsheet.pdf
Instructions.pdf
TLP-WHITE-Botconf2018-MISP_CTI_Info_Sharing.pdf
TLP-WHITE-Botconf2018-WS3-MISP_TheHive_Cortex.pdf

TheHive-Cortex-MISP-Workshop/Training VMs:
apikeys.txt
packer_virtualbox-iso_virtualbox-iso_sha256.checksum
report-templates.zip
thehive-misp.ova
```

Import the Training VM

While TheHive Project and MISP Project provide separate training VMs, one including only TheHive and Cortex and another including only MISP, both projects have worked together in order to provide a unified VM which contains all three applications for their regular joint workshops and trainings such as this one.

The USB keys provided by the instructors contain the latest unified training VM, in the `Training VMs` folder:

`thehive-misp.ova`

The unified training VM works on both VirtualBox and VMware Workstation/Fusion. **Please do not use VMware Player** as problems might occur with that application.

Important Note

The training VMs must not be used for production systems. Their only purpose is to help you get acquainted with the applications.

Before importing the VM in your virtualization software, please check its SHA256 fingerprint against the hash stored in:

```
Training VMs/packer_virtualbox-iso_virtualbox-iso_sha256.checksum
```

If fingerprints do not match, call the instructors. Otherwise, proceed and import the VM in VirtualBox or VMware. **Please allocate 6GB of RAM to it and at least 2 processor cores if you can**. 4GB is a bare minimum.

CLI/SSH

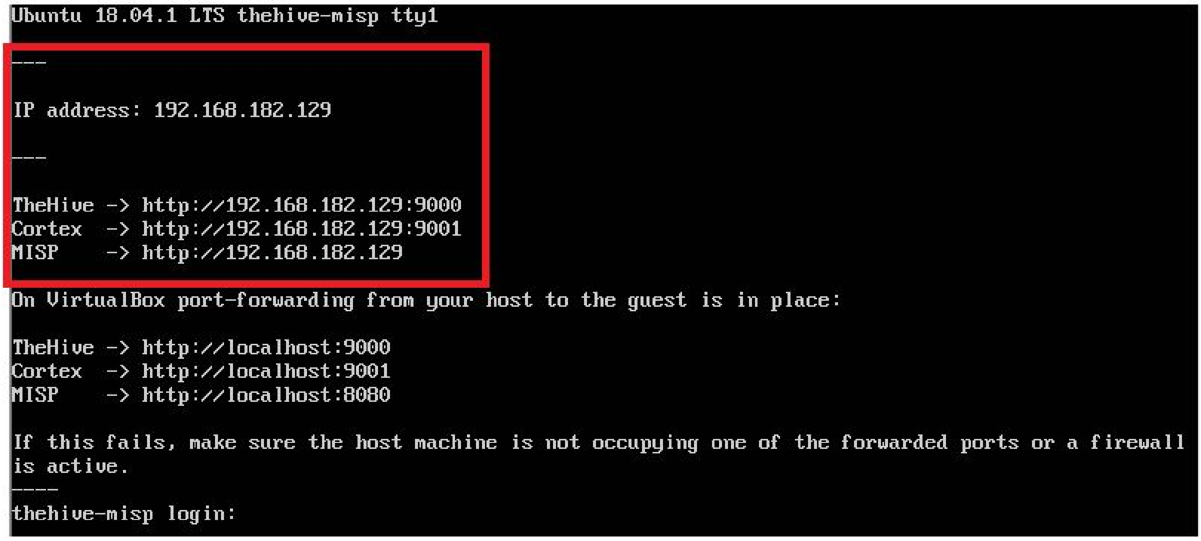
To connect to the VM through SSH or the CLI, use the `misp` user account with password `Password1234`.

Set up MISP

Step 1 – Connect to the MISP Web UI

VMware

When the VM finishes booting up, it will display the following banner:



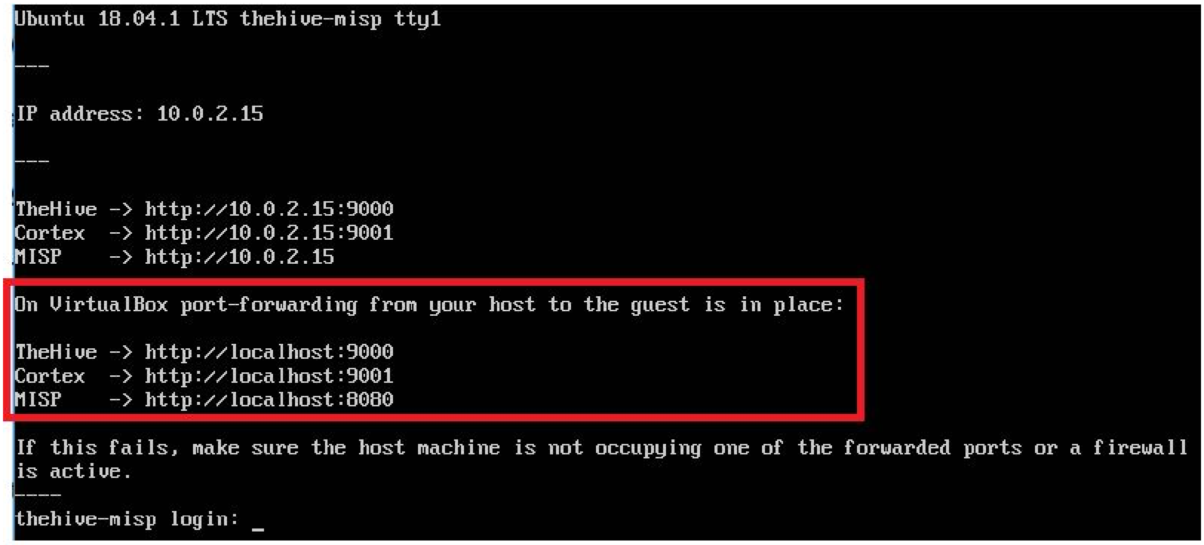
```
Ubuntu 18.04.1 LTS thehive-misp tty1

---

IP address: 192.168.182.129

---

TheHive -> http://192.168.182.129:9000
Cortex  -> http://192.168.182.129:9001
MISP    -> http://192.168.182.129
On VirtualBox port-forwarding from your host to the guest is in place:

TheHive -> http://localhost:9000
Cortex  -> http://localhost:9001
MISP    -> http://localhost:8080

If this fails, make sure the host machine is not occupying one of the forwarded ports or a firewall
is active.
----
thehive-misp login:
```

Launch a browser on your host machine and connect to:

http://JOINT_VM_IP (VMware)

In the screenshot above, the URL is http://192.168.182.129. **Use the one indicated in your own banner**. Login as `admin@admin.test` with password `admin`.

Virtualbox
When the VM finishes booting up, it will display the following banner:



```
Ubuntu 18.04.1 LTS thehive-misp tty1

---

IP address: 10.0.2.15

---

TheHive -> http://10.0.2.15:9000
Cortex  -> http://10.0.2.15:9001
MISP    -> http://10.0.2.15

On VirtualBox port-forwarding from your host to the guest is in place:

TheHive -> http://localhost:9000
Cortex  -> http://localhost:9001
MISP    -> http://localhost:8080

If this fails, make sure the host machine is not occupying one of the forwarded ports or a firewall
is active.
----
thehive-misp login: _
```

As indicated, port-forwarding is already configured and as such you can access MISP by launching a browser on your host machine and connect to:

http://localhost:8080

Login as `admin@admin.test` with password `admin`.

Step 2 – Change the Base URL

This is very important.

Change the base URL of your MISP instance via *Administration > Server Settings & Maintenance > MISP Settings > MISPbaseurl* to correspond to the URL you used to connect to MISP.

Step 3 – Sync MISP

Your instructors will share with you the URL of a MISP instance containing several hundred of events. It is time to sync your training instance with it.

To do so, go to *Sync Action > List Servers* then click on *New Server*. In the *Base URL* field, type:

http://IP_ADDR_GIVEN_BY_TRAINERS:8080

In the *Instance Name* field, type:

MISP-HONEYLOVE

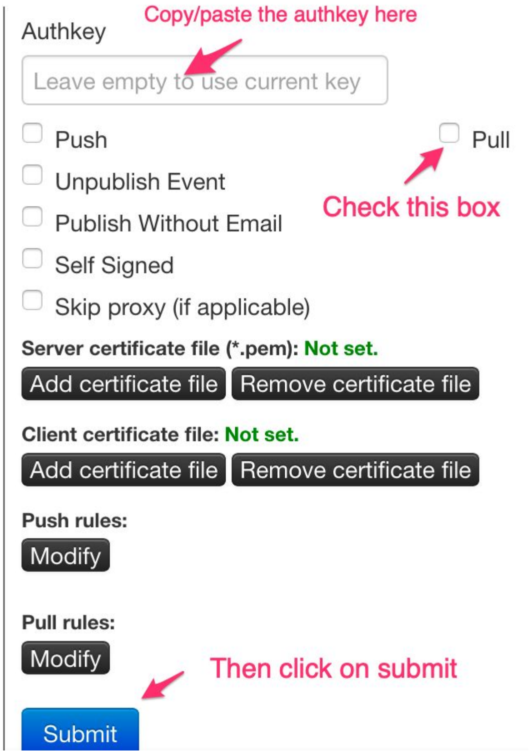
Then copy the following key and paste it in the *Authkey* field:

io1juTxLMOu1e24qddKQ3IM6HTw8El5NiZ8jg2mz

Important Note

Do not type the authentication key's value (the long string corresponding to the `Authkey` field) by hand. Please copy/paste it from the `Training VMs/apikeys.txt` file or from this document (see the value above).

Check the *pull* box and click on *Submit*:



Authkey

Leave empty to use current key

□ Push

□ Unpublish Event

□ Publish Without Email

□ Self Signed

□ Skip proxy (if applicable)

□ Pull

Server certificate file (*.pem): Not set.

Add certificate file | Remove certificate file

Client certificate file: Not set.

Add certificate file | Remove certificate file

Push rules:

Modify

Pull rules:

Modify

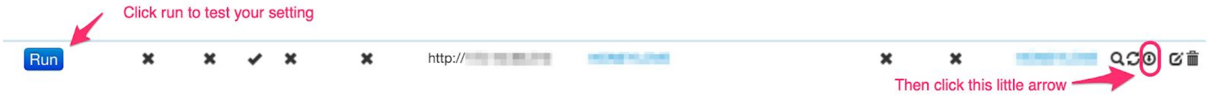
Submit

Copy/paste the authkey here

Check this box

Then click on submit

To test your setup, click on the **Run** button next to the server name/IP. Then look at the added server and **click on the little *down arrow* located on the right side of the display to pull all events**.



Run ✖ ✖ ✔ ✖ ✖ http:// ✖ ✖

Click run to test your setting

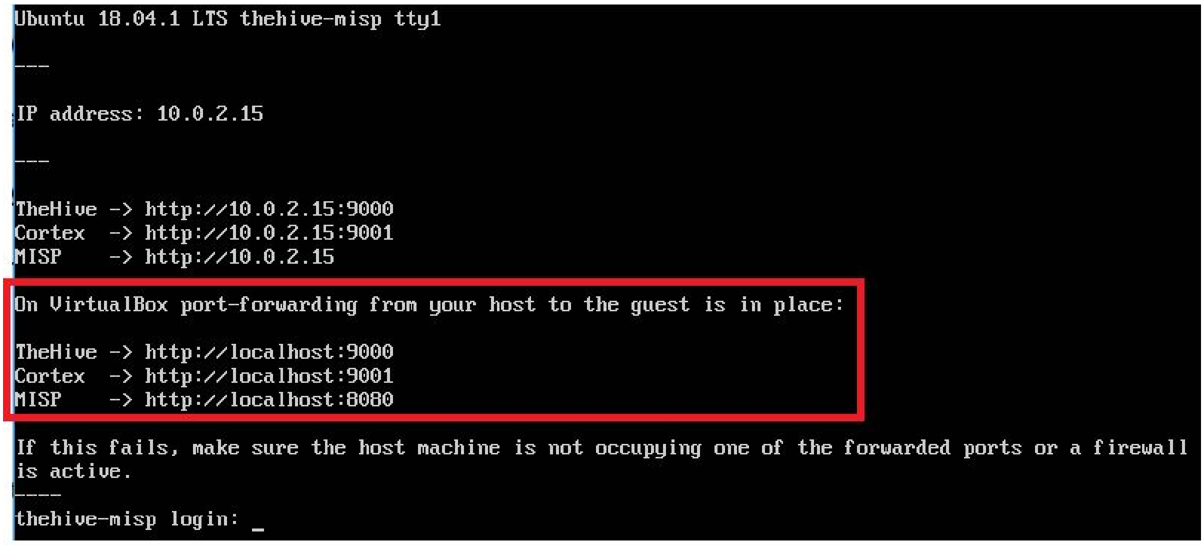
Then click this little arrow

Wait a few minutes and click on *Home* on the top left side of the Web UI. You should see some events.

Set up TheHive & Cortex

Step 1 - Connect to TheHive's Web UI

Look at the banner of your VM:



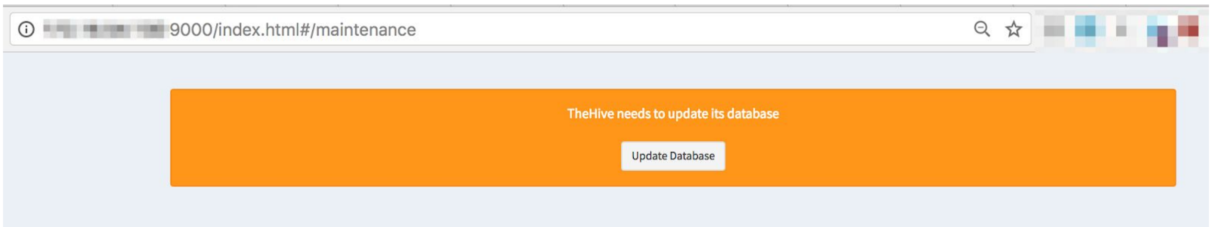
```
Ubuntu 18.04.1 LTS thehive-misp tty1

---

IP address: 10.0.2.15

---

TheHive -> http://10.0.2.15:9000
Cortex  -> http://10.0.2.15:9001
MISP    -> http://10.0.2.15

On VirtualBox port-forwarding from your host to the guest is in place:

TheHive -> http://localhost:9000
Cortex  -> http://localhost:9001
MISP    -> http://localhost:8080

 If this fails, make sure the host machine is not occupying one of the forwarded ports or a firewall
 is active.
----
thehive-misp login: _
```

Launch a browser on your host machine and connect to:

http://JOINT_VM_IP:9000 (VMware)

http://localhost:9000 (VirtualBox)

In a real-world scenario, the first time you access TheHive, you'll need to create the associated database by clicking on the `Update Database` button as shown below:



[redacted]9000/index.html#/maintenance

TheHive needs to update its database

Once this is done, you'll be asked to create an admin account with an associated password.

For the workshop, the steps below have already been done in advance and does not require actions from your side:

- Database creation
- Admin account creation

To connect to TheHive's Web UI, use the account `admin` with password `thehive1234`. Now open a session on TheHive using those credentials and **explore the UI**. Take your time and please ask questions to the instructors when something is unclear.

Step 2 - Connect to the Cortex Web UI

On your host machine, connect to:

http://JOINT_VM_IP:9001 (VMware)

http://localhost:9001 (VirtualBox)

While TheHive has only one administrator account level (either you have admin privileges or you haven't), Cortex supports RBAC or multi-tenancy and allows you to manage multiple organizations within a single instance. Cortex has two administrator account levels:

- Super administrators: *superadmins* can create, modify or remove organizations and user accounts. They cannot see what's happening within a specific organization nor manage its responders and analyzers.
- Organization administrators: *orgadmins* can manage users within their own organizations, enable and configure analyzers, quotas and caching.

First, start by opening a session as a *super administrator* using the `admin` account with `thehive1234` as a password. **Explore the UI**. Take your time and please ask questions to the instructors when something is unclear.

Log out and log back in using an *organization administrator* account. The username is `thehive` and the password is `thehive1234`. **Explore now the interface** and see how different it is from the previous display when you were connected using a super administrator account. Take your time and please ask questions to the instructors when something is unclear.

Step 3 (OPTIONAL) – Update Your Cortex Analyzers

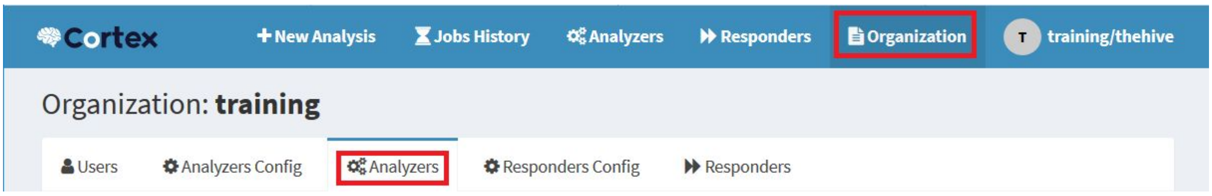
This step is not required for the workshop as you already have the latest analyzers.

To install the latest analyzers and fixes, open a shell on the training VM (hint: use SSH from your host OS or CLI; login: `misp` & password: `Password1234`) and run the following commands:

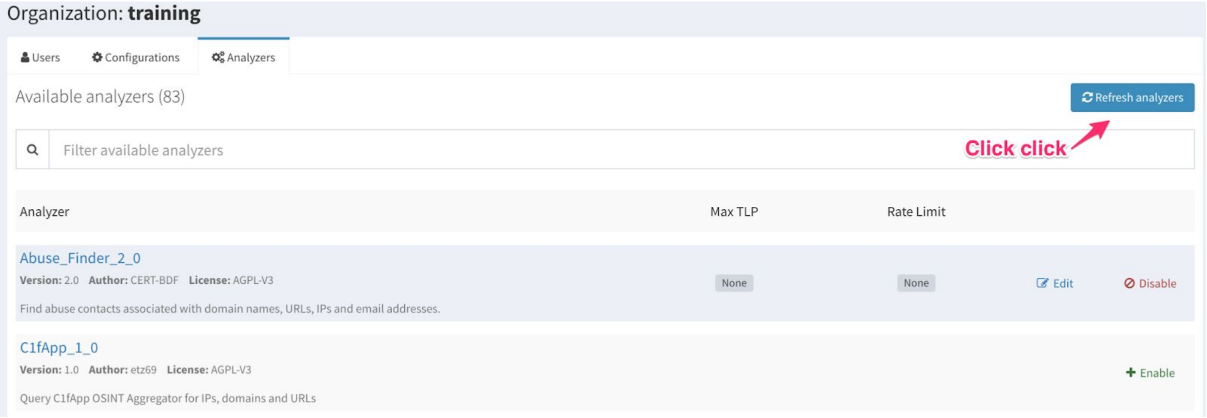
```
$ cd /opt/Cortex-Analyzers
$ sudo git pull
$ for I in analyzers/*/requirements.txt; do sudo -H pip2 install -r
$I; done && \
for I in analyzers/*/requirements.txt; do sudo -H pip3 install -r $I
|| true; done
```

They might take some time to complete.

On The Cortex UI, log in as `thehive` with password `thehive1234`. In the navigation bar, click on *Organization*, then *Analyzers*:



Finally, click on *Refresh Analyzers* as shown below:

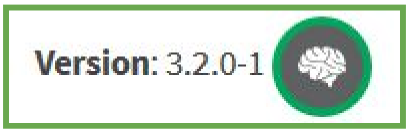


Analyzer	Max TLP	Rate Limit		
Abuse_Finder_2_0 Version: 2.0 Author: CERT-BDF License: AGPL-V3 Find abuse contacts associated with domain names, URLs, IPs and email addresses.	None	None	Edit	Disable
C1fApp_1_0 Version: 1.0 Author: etz69 License: AGPL-V3 Query C1fApp OSINT Aggregator for IPs, domains and URLs				Enable

Step 4 – Check the Local Cortex Connectivity

This step needs to be performed on TheHive.

TheHive is already configured to leverage the Cortex instance that is included in the training VM. To make sure that's the case, check the Cortex logo at the lower bottom of TheHive's main page. It should have an outer circle in `green` color :



If that's not the case, please refresh the page and check again. If that still does not work, open a shell on the VM using `misp` user account with Password1234 as a password then type:

```
$ sudo service thehive stop
$ sudo service thehive start
```

Go back to your host's browser, open a session on TheHive and check again the color of the outer circle surrounding the Cortex logo. It should be green now.

Step 5 – Import the Report Templates

The Cortex instance is pre-configured with the following 6 analyzers:

- Abuse Finder
- CyberCrime-Tracker
- EmlParser
- Fortiguard URLCategory
- MaxMind GeoIP
- UnshortenLink

Have a look at TheHive's report templates: go to *Admin > Report templates* menu. How many templates do you see ?

Now connect as an *orgadmin* user on the Cortex UI (user: `thehive`, password: `thehive1234`) and enable the FileInfo analyzer: *Organization > Analyzers > FileInfo_5_0 > Enable*. **Set all *manalyze* configuration to False**, keep *Options* as default and save.

Go back to TheHive's report templates and refresh the page. Do you notice something different? The available report templates should have been updated automatically to include *FileInfo_5_0*. If not, the report templates must be reinstalled in TheHive in order to fully benefit from all the analyzers.

To do so:

1. In TheHive, go to *Admin > Report templates* menu.
2. Click on the *Import templates* button and select the file `Training VMs/report-templates.zip` you copied from the USB key. Alternatively, you can also download it online from the following location: https://dl.bintray.com/thehive-project/binary/report-templates.zip

Important Note

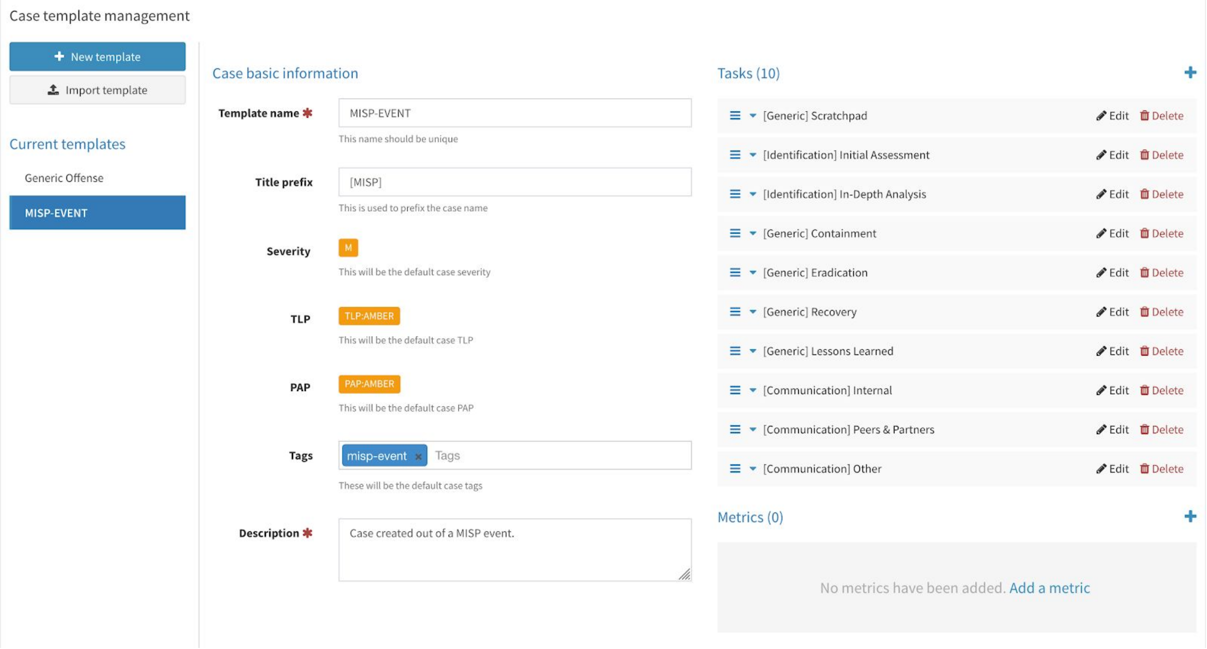
You will need the *FileInfo_5_0* analyzer for the case studies. But due to a recent change in a library it uses, it does not work out of the box. We will be fixing this issue shortly. In the meantime, **please open a shell on your training VM and issue the following commands**:

```
 $ sudo -H pip3 uninstall extract-msg
[press y]
$ sudo -H pip2 uninstall extract-msg
[press y]
$ sudo -H pip2  install \
git+https://github.com/mattgwwalker/msg-extractor.git@v0.19
$ sudo -H pip3  install \
git+https://github.com/mattgwwalker/msg-extractor.git@v0.19
```

Step 6 – Configure TheHive & MISP Integration

In TheHive's Web UI, go to the *Admin > Case template* menu and **create a case template** that will be used to import MISP events of interest as cases to investigate by default. Call it **MISP-EVENT**.

Here is an example. Note that you can create **task groups:**



Case template management

Current templates
- Generic Offense
- MISP-EVENT

Case basic information

Template name *: MISP-EVENT
This name should be unique

Title prefix: [MISP]
This is used to prefix the case name

Severity: M
This will be the default case severity

TLP: TLP:AMBER
This will be the default case TLP

PAP: PAP:AMBER
This will be the default case PAP

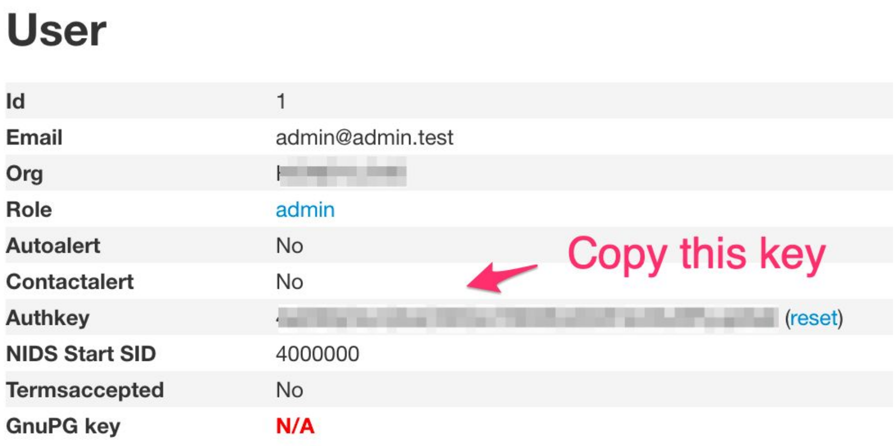
Tags: misp-event
These will be the default case tags

Description *: Case created out of a MISP event.

Tasks (10)
- [Generic] Scratchpad
- [Identification] Initial Assessment
- [Identification] In-Depth Analysis
- [Generic] Containment
- [Generic] Eradication
- [Generic] Recovery
- [Generic] Lessons Learned
- [Communication] Internal
- [Communication] Peers & Partners
- [Communication] Other

Metrics (0)
No metrics have been added. Add a metric

Connect to your MISP VM's Web UI using `admin@admin.test` with password `Password1234`. Click on *Admin* on the right side of the top navigation bar. Copy the value of the *Authkey* field.



User

Id	1
Email	admin@admin.test
Org	[redacted]
Role	admin
Autoalert	No
Contactalert	No
Authkey	[redacted] (reset)
NIDS Start SID	4000000
Termsaccepted	No
GnuPG key	N/A

Copy this key

Important Note

> In real-world situations, you must not use a MISP's admin `Authkey` for TheHive. Instead, you should create a Sync user account for TheHive in the MISP Web UI and use the associated `Authkey` in TheHive's configuration.

Open a shell on your training VM and edit TheHive’s configuration file located at:

```
/etc/thehive/application.conf
```

Edit the *MISP* section of the configuration file to look like the following.

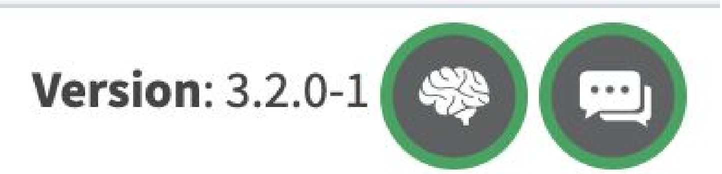
```
## Enable the MISP module (import and export)
play.modules.enabled += connectors.misp.MispConnector

misp {
  # Interval between consecutive MISP event imports in hours (h)
or
  # minutes (m).
  interval = 1h

  "MISP-LOCAL" {
  #  # MISP connection configuration requires at least an url and a
key. The key must
  #  # be linked with a sync account on MISP.
      url = "http://localhost" # Yes, localhost, not localhost:8080
      key = "Your Authkey goes here"
  #
  #  # Name of the case template in TheHive that shall be used to
import
  #  # MISP events as cases by default.
      caseTemplate = "MISP-EVENT"
  #
  #  # Optional tags to add to each observable imported from an
event
  #  # available on this instance.
      tags = ["misp-local"]
  #
  #  ## MISP event filters
  #  # MISP filters is used to exclude events from the import.
  #  # Filter criteria are:
  #  # The number of attribute
  #  max-attributes = 1000
  #  # The size of its JSON representation
  #  max-size = 1 MiB
  #  # The age of the last publish date
  #  max-age = 7 days
  #  # Organization and tags
  #  exclusion {
  #   organisation = ["bad organisation", "other orga"]
  #   tags = ["tag1", "tag2"]
  #  }
  #
  #  ## HTTP client configuration (SSL and proxy)
  #  # Truststore to use to validate the X.509 certificate of the
MISP
  #  # instance if the default truststore is not sufficient.
  #  # Proxy can also be used
  #  ws {
  #   ssl.trustManager.stores = [ {
  #   path = /path/to/truststore.jks
  #   }
  #   proxy {
  #   host = proxy.mydomain.org
  #   port = 3128
  #   }
  #  }
  #
  #  # MISP purpose defines if this instance can be used to import
events (ImportOnly), export cases (ExportOnly) or both
(ImportAndExport)
  #  # Default is ImportAndExport
  #  purpose = ImportAndExport
  } ## <-- Uncomment to complete the configuration
}
```

Save the file and restart TheHive:

```
$ sudo service thehive restart
```

Open a session on TheHive's Web UI using admin and password thehive1234:

1. Check that you have now the MISP logo in the lower right corner of the main page once you have authenticated to TheHive. If not, call us for help.



2. Notice how the value next to the *Alerts* navigation item is increasing. You can also force the synchronization **if needed** by accessing the following URL:
http://JOINT_VM_IP:9000/api/connector/misp/_syncAlerts (VMware)

   http://localhost:9000/api/connector/misp/_syncAlerts (VirtualBox)

Step 7 – Configure an additional Cortex Instance

It is time to add an additional Cortex instance to TheHive's configuration. It will allow you to test additional subscription-based and commercial analyzers and work more efficiently on the case study.

Open a shell on TheHive's training VM and edit TheHive's configuration file located at:

```
/etc/thehive/application.conf
```

Look for the Cortex configuration section. It should look like:

```
# Cortex
# TheHive can connect to one or multiple  Cortex  instances.  Give
each
# Cortex instance a name and specify the associated URL.
play.modules.enabled += connectors.cortex.CortexConnector
cortex {
  "LOCAL CORTEX" {
    # URL of the Cortex server.
    url = "http://127.0.0.1:9001"
    key ="some API key goes here"
  }
}
```

Now configure TheHive to access an additional Cortex instance.

Important Note

Do not type the authentication key's value (the long string corresponding to the `key` variable) **by hand**. You can find it in the `Training VMs/apikeys.txt` file you copied from the USB key. Please open an SSH connection from your host OS to your guest OS and copy/paste the key from the `apikeys.txt` file to the `key`'s value shown below in `/etc/thehive/application.conf`.

```
# Cortex
# TheHive can connect to one or multiple Cortex instances. Give each
# Cortex instance a name and specify the associated URL.
play.modules.enabled += connectors.cortex.CortexConnector
cortex {
  "LOCAL CORTEX" {
    # URL of the Cortex server.
    url = "http://127.0.0.1:9001"
    key ="some API key goes here"
  }
  "CORTEX-HONEYLOVE" {
    # URL of the Cortex server.
    url = "http://CORTEX_URL_SHARED_BY_THE_INSTRUCTORS_GOES_HERE"
    key ="jDpWqnpJBgSHtD5mlP72BZV3gcfadLFH"
  }
}
```

Save the file and restart TheHive:

```
$ sudo service thehive restart
```

Connect to TheHive's Web UI, click on your username on the right side of the top navigation bar then on *About TheHive*. You should see two Cortex instance names, along with their version and their status.

Case Studies

Case 1: Your Car is Waiting

You are the incident handler on duty for the HoneyLove company which is incorporated in Luxembourg for obvious reasons. Joe Smith is your CEO's assistant. Your CEO travels a lot to sell the delicious honey produced by HoneyLove. So Joe is often planning your boss' trips. He purchases airplane tickets, books hotel rooms and cars etc. His life consists of dealing with emails and phone calls mostly.

As he is going through tons of emails, he spots one in his mailbox that seems a bit weird. The subject is the following:

> [Avis Business Club] Booking Confirmation Email

It is true that HoneyLove works exclusively with Avis for car rental and as a very successful company (honeybees are getting very rare so the price of honey has skyrocketed in the last couple of years), HoneyLove is member of Avis Business Club. It is also true that Joe often receives such emails but the sender and contents of the email are unusual this time.

Joe calls you and you asked him to drag/drop the email on his desktop. This created an EML file. Then you asked him to send you the EML file which he did. The EML file is now on your regular workstation in `Case\ Studies/Case1-JoeSmith`.

It's investigation time! Create a case in TheHive (**hint:** prepare a case template for suspicious email investigations), add the EML file as observable and fire the EML Parser analyzer. Look at the results carefully. Add new observables from the report (sender, recipient, subject, URL, domain…).

Notice that there is an attachment. It's a password-protected ZIP file. You should extract it from the EML file before adding it to your case. You can use the old `vi/nano` method **or install `mpack`** on your training VM, copy the EML file there and extract the attachment:

> https://ubuntuincident.wordpress.com/2010/09/27/extract-email-attachments/

Be careful once you have the attachment on your workstation. **You can upload the password-protected ZIP file directly to TheHive without having to decrypt it beforehand**. All you need is the password. Look again at the EML Parser analyzer report.

Fire some additional analyzers. Think wisely. Can you find additional IOCs in the analyzer reports? What are your conclusions? Is it a true positive? Close the case once finished and, if it is a true positive and you have identified some IOCs, use the *Share* button to push them to your MISP instance then connect to the MISP Web UI and verify that the case has been correctly exported. Note that the event is not published as it requires sanitization by the threat intel team before publication (and sharing with peers and partners if applicable).

Case 2: Feed me an Alert

You've been dealing with user notifications using the *copy/paste/send* method outlined in case 1 for quite some time. It is tedious for your users. It is tedious for you and it is a waste of time.

As a good (i.e. lazy) incident handler, you are looking into automating things. TheHive has the ability to receive alerts from multiple sources using simple Python programs called Alert Feeders.

HoneyLove uses Google for emails. You asked your I.T. department to add a button on the mail clients to report suspicious emails to your team.

When a user spots a suspicious email, they highlight it and click on the button then click on send after adding an optional comment. The email is packaged as an EML file and sent to a mailbox monitored by an alert feeder.

In this case study, you will have to create a basic alert feeder that will extract key data from EML files and feed it to TheHive as an alert.

Samantha Fox works in the procurement department of HoneyLove after a brief career in the show business. She just received an email which subject is:

> ACH Payment info

The email apparently comes from Enovos Luxembourg SA from which HoneyLove gets its electricity but something is off.

Samantha clicks on the 'report email' button and the EML file lands in the mailbox monitored by your alert feeder. Copy Case 2 data to your TheHive VM:

```
❯ ls -l Case\ Studies/Case2-AlertFeeder
total 368
-rw-r--r--@ 1 saad  staff  181211 Oct 16 23:03 ACH Payment info.eml
-rwxr-xr-x@ 1 saad  staff    1994 Oct 16 23:26 email-alert.py
```

On your TheHive VM, edit the EML file and look if there's an attachment. If there's one, you may want to extract it using `munpack` as you might have done in case 1.

Edit `email-alert.py` and customize it. You need an API key:

1. Go to TheHive's Web UI
2. Click on *Admin > Users*
3. Create an account for your alert feeder (check the *Allow alerts creation checkbox*)
4. Give it *read* rights (you don't need to give alert feeders any right apart from alert creation in production but for the workshop it is required)
5. Generate an API key for that account

Make sure to populate your artifacts correctly, add tags, descriptions if needed etc. When you are ready, execute the alert feeder. The alert should show up in TheHive. Preview it, import it and start investigating. Use analyzers & so on. What is your conclusion? Is it malicious?

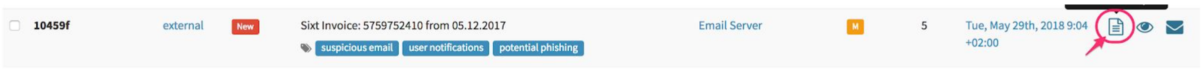
Spoiler Alert

If you are stuck, you can look at a working example that needs very little customization here: https://drive.google.com/file/d/1LhjKWWh3ddW6j7GLJYpm9OTKOW4wX_Uf/view?usp=sharing

If you end generating an incorrect alert, you can mark it as read (easy way). But you can also delete it using the following command (complicated way) on the training VM:

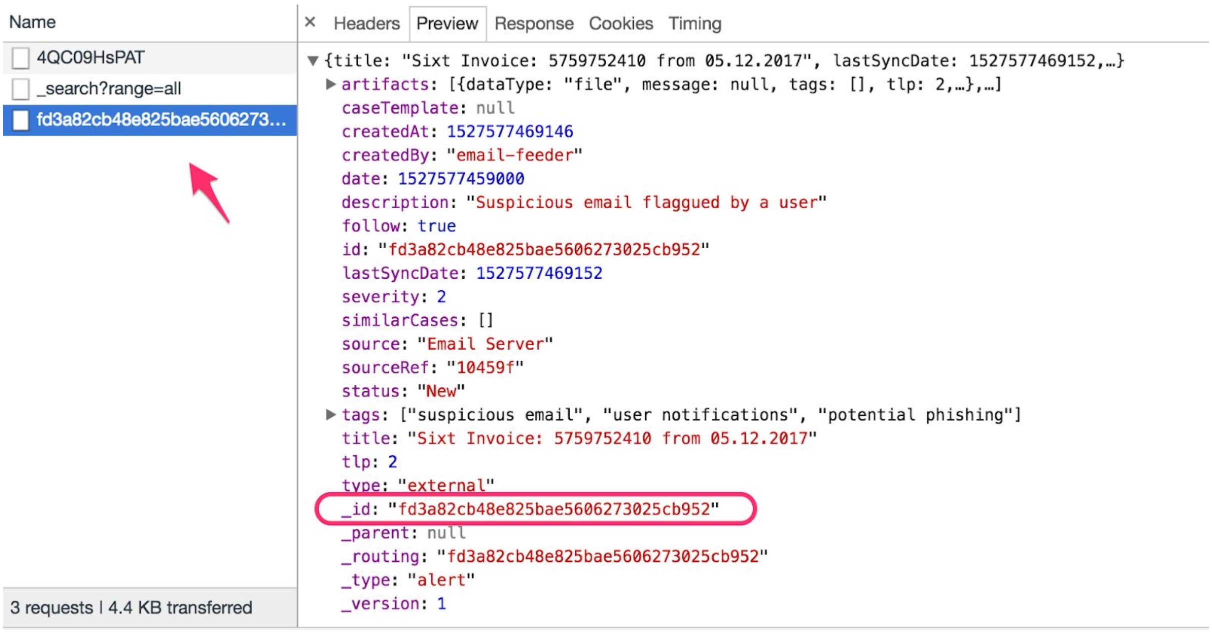
```
curl -XDELETE http://localhost:9200/the_hive_14/alert/ID
```

To get the **ID**, use your browser's web console, preview the alert in the UI and catch the request



□ 10459f	external	New	Sixt Invoice: 5759752410 from 05.12.2017 suspicious email user notifications potential phishing	Email Server	M	5	Tue, May 29th, 2018 9:04 +02:00

Then grab the ID:



Name
4QC09HsPAT
_search?range=all
fd3a82cb48e825bae5606273...
3 requests | 4.4 KB transferred
× Headers Preview Response Cookies Timing

```
▼{title: "Sixt Invoice: 5759752410 from 05.12.2017", lastSyncDate: 1527577469152,…}
  ▶artifacts: [{dataType: "file", message: null, tags: [], tlp: 2,…},…]
   caseTemplate: null
   createdAt: 1527577469146
   createdBy: "email-feeder"
   date: 1527577459000
   description: "Suspicious email flagguęd by a user"
   follow: true
   id: "fd3a82cb48e825bae5606273025cb952"
   lastSyncDate: 1527577469152
   severity: 2
   similarCases: []
   source: "Email Server"
   sourceRef: "10459f"
   status: "New"
  ▶tags: ["suspicious email", "user notifications", "potential phishing"]
   title: "Sixt Invoice: 5759752410 from 05.12.2017"
   tlp: 2
   type: "external"
   _id: "fd3a82cb48e825bae5606273025cb952"
   _parent: null
   _routing: "fd3a82cb48e825bae5606273025cb952"
   _type: "alert"
   _version: 1
```

If you want to remove permanently all the alerts from your instance, use the following command on the training VM:

```
curl -XPOST http://localhost:9200/the_hive_14/_delete_by_query -d '{
    "query":
    {
    "match": {"_type":"alert"}
    }
    }'
```

Case 3: Knock, Knock, you've got an Event

Once you reached this point, please state so to the instructors.

One of your peer CSIRTs just published on their MISP instance an interesting event. You force a pull on your MISP instance to get it. Start by exploring the event in MISP. You can use expansion modules if you need to enrich the data.

Since you don't want to wait for the 1h interval time to see it in TheHive, use the magic URL:

http://JOINT_VM_IP:9000/api/connector/misp/_syncAlerts (VMware)

http://localhost:9000/api/connector/misp/_syncAlerts (VirtualBox)

It's investigation time again! Do you see something related to a previous case you dealt with?

Good luck and if you find some new IOCs, share them back on MISP!

Before you Leave

We always welcome feedback to help us improve MISP, TheHive, Cortex and their integration. We also appreciate your feedback on our trainings & workshops to make them better and more useful for future attendees. Last but not least, if you have questions or comments, feel free to contact us:

- By email: support@thehive-project.org
- By joining our user forum (Google Group)
- By chatting with us and our user community on Gitter

This is a community-led effort and your contributions (new analyzers, new responders, UX improvements, feature requests, …) will help us all.

Thank you!