Incident Response in The Age of Cyber Threat Intelligence Training

With TheHive, Cortex & MISP
30th Annual FIRST Conference
Kuala Lumpur, Sunday June 24, 2018

Dear Training Attendees,

Before coming to the classroom, you should download and install the MISP and TheHive/Cortex training VMs for the training as described in the steps below. We also have a small number of USB keys from which you may copy them if you failed to do so before the event.

During our day together, we should be able to cover the following:

- What is Incident Response and Cyber Threat Intelligence in 2018
- Overview of the software stack
- Simple case study
- Dealing with notifications
- How CTI feeds IR
- How IR feeds CTI
- Advanced case study.

We should be able to give you access to:

- A Cortex server configured with several subscription-based/commercial analyzers such as DomainTools, CIRCL pSSL/pDNS & so on.
- A MISP instance that contain several hundreds of events to either connect TheHive to directly and/or synchronize with your own training MISP application.

Table of Contents

MISP

Step 1 – Download the training VM

If you are running VMware, download the VM from the following location:
https://www.circl.lu/misp-images/MISP_v2.4.90@f0dbdb70708bc84e39e2f9f271db7ede411be81a/MISP_v2.4.90@f0dbdb70708bc84e39e2f9f271db7ede411be81a-vmware.zip

Otherwise, if you are running VirtualBox:
https://www.circl.lu/misp-images/MISP_v2.4.90@f0dbdb70708bc84e39e2f9f271db7ede411be81a/MISP_v2.4.90@f0dbdb70708bc84e39e2f9f271db7ede411be81a.ova

Alternative option: get it from one of the USB keys provided during the training.

Step 2 – Check the VM SHA256 fingerprint

```
9e886fb80ab125c675527c1f3bd2470f772e78ee8f2b80be875981764bdb6410
MISP_v2.4.90@f0dbdb70708bc84e39e2f9f271db7ede411be81a-vmware.zip
```

```
d4add96601ba3027a59d26850579f2e15591ba60968566524ce403f42eb0de76
MISP_v2.4.90@f0dbdb70708bc84e39e2f9f271db7ede411be81a.ova
```

Step 3 – Connect to the MISP Web UI

Launch the VM in your virtualization software then connect to the VM's CLI using the `misp` user account with password `Password1234`. Get your VM IP address using `ifconfig` and write it down.

Launch a browser on your host machine and connect to:
http://YOUR_MISP_VM_IP_ADDR

Login as admin@admin.test with password admin.

Step 4 – Change the base URL

Change the base URL of your MISP instance via *Administration > Server Settings & Maintenance > MISP Settings > MISPbaseurl* to correspond to the IP address of your VM.

Step 5 – Update MISP

Update your MISP instance to version 2.4.92 via the *Administration > Server Settings & Maintenance > Diagnostics > Update MISP* button. Wait for the update to complete. You should now have version 2.4.92.

Step 6 – Sync MISP

The trainers should have shared with you the URL of a MISP instance containing several hundred of events. It is time to sync your training instance with that one.

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:9080

In the *Instance Name* field, type:

MISP-NSEC

Then in the *Authkey* field, provide the following key:

Rc6ppkFPKVIS6OI7sSF43XJtJbcVoPjdXInTPecT

Check the *pull* box and click on *Submit*. 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. Wait

TheHive & Cortex

Step 1 – Download the training VM

Download the training VM from:
https://drive.google.com/open?id=0B3G-Due88gfQMzlfZ2t6RVhqTUk

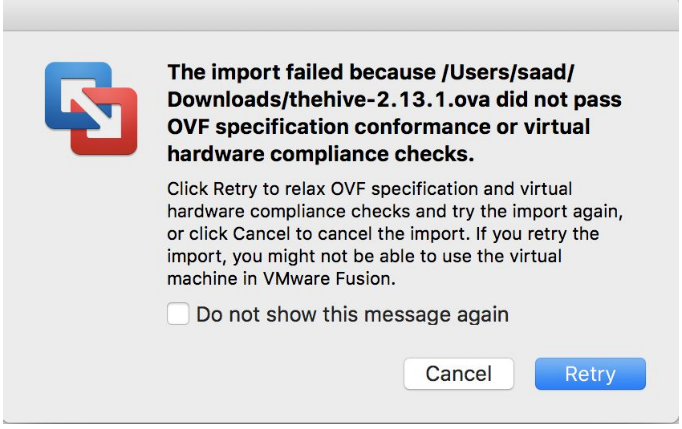
Alternative option: get it from one of the USB keys provided during the training.

Step 2 – Check the VM SHA256 fingerprint

```
b5be8c927f37a975a8050d57e907a5b49a090d0dbe21b4b17766d5e10756a673
thehive-training-3.0.10.ova
```

Step 3 – Connect to TheHive and Cortex Web UIs

Launch the VM in your virtualization software. VirtualBox and VMware Workstation/Fusion should work nicely. If you get an error like the one below, you can safely ignore it and click on *Retry*:



The import failed because /Users/saad/Downloads/thehive-2.13.1.ova did not pass OVF specification conformance or virtual hardware compliance checks.

Click Retry to relax OVF specification and virtual hardware compliance checks and try the import again, or click Cancel to cancel the import. If you retry the import, you might not be able to use the virtual machine in VMware Fusion.

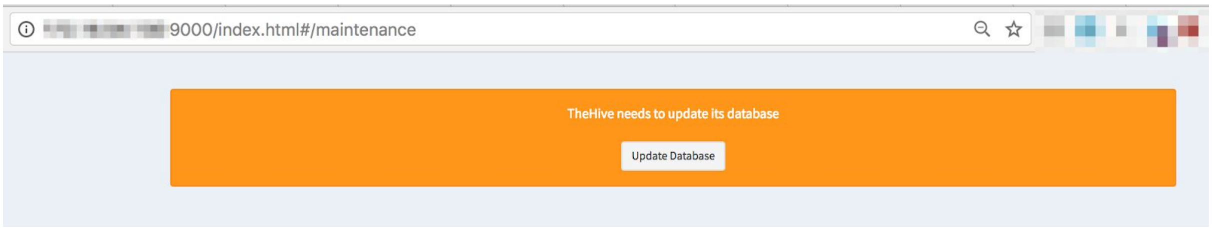
□ Do not show this message again

Once your VM is started, its console should display the URLs of TheHive and Cortex. Write them down. Alternatively, you may connect to the VM's CLI using the `thehive` user account with password `thehive1234` then obtain your VM IP address using ifconfig and write it down.

TheHive

Launch a browser on your host machine and connect to:
http://YOUR_THEHIVE_VM_IP_ADDR:9000

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. **Make sure to save those credentials somewhere as you'll need them later**.

Now open a session on TheHive using those credentials.

Cortex

On your host machine, connect to:
http://YOUR_THEHIVE_VM_IP_ADDR:9001

Open a session as a super administrator using the `admin` account with `thehive1234` as a password. Explore the interface. 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.

Step 3 – Check local Cortex connectivity

TheHive's training VM includes Cortex and TheHive is configured to leverage it. To make sure that's the case, check the Cortex logo at the lower bottom of the 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 `thehive` user account with `thehive1234` 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 4 – Import the report templates

The training VM is delivered with *Abuse Finder*, *File_Info*, *Msg_Parser* and *MaxMind GeoIP* enabled.
To fully benefit from the analyzers, you should install the associated report templates in TheHive:

- Download the report template package: https://dl.bintray.com/cert-bdf/thehive/report-templates.zip
  Alternative option: get it from the USB keys provided during the training
- In TheHive, go to *Admin > Report templates* menu
- click on the *Import templates* button and select the downloaded package

Step 5 – 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.

In MISP's Web UI, connect 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.

Open a shell on TheHive's 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 {
  "MISP-training" {
    # URL of the MISP instance.
    url = "http://IP_ADDR_OF_YOUR_MISP_VM"

    # Authentication key.
    key = "Authkey value you copied in the previous step"

      # Name of the case template in TheHive that shall be used to
import
    # MISP events as cases by default.
    caseTemplate = "MISP-EVENT"

       # Tags to add to each observable imported from an event
available on
    # this instance.
    tags = ["misp-training"]

     # Truststore to use to validate the X.509 certificate of the
MISP
    # instance if the default truststore is not sufficient.

    #ws.ssl.trustManager.stores =  [
  #{
  #  type: "JKS"
  #  path: "/path/to/truststore.jks"
  #}
  #]
 }

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

Save the file and restart TheHive:

```
$ sudo service thehive restart
```

Open a session on TheHive's Web UI and notice how the value next to the *Alerts* navigation item is increasing.

Open a shell on TheHive's training VM and look for lines that resemble the following in */var/log/thehive/application.log*:

```
2018-05-15  14:33:49,952  [INFO]  from  connectors.misp.MispConnection
in main - Add MISP connection MISP-training
  url:              http://MISP-VM-IP-ADDR
  proxy:            None
  case template:    MISP-EVENT
  artifact tags:    misp-t
raining filters:
    max age:        <not set>
    max attributes: <not set>
    max size:       <not set>
    excluded orgs:
    excluded tags:

2018-05-15  14:33:50,014  [INFO]  from  connectors.misp.MispSynchro  in
application-akka.actor.default-dispatcher-5 - Update  of  MISP  events
is starting ...
2018-05-15    14:33:50,329    [INFO]    from    play.api.Play    in
main - Application started (Prod)
2018-05-15  14:33:50,360  [INFO]  from  connectors.misp.MispSynchro  in
application-akka.actor.default-dispatcher-7 - Synchronize        MISP
MISP-training from Some(Thu Jan 01 00:00:00 UTC 1970)
[...]
2018-05-16  02:55:17,450  [INFO]  from  connectors.misp.MispSynchro  in
application-akka.actor.default-dispatcher-390 - Misp  synchronization
completed
```

Important note:
During the training, if you create or update MISP events and want them to show up immediately in TheHive's alert panel, use the following URL to force synchronization:

http://YOUR_THEHIVE_VM_IP_ADDR:9000/api/connector/misp/_syncAlerts

Step 6 – Configure an additional Cortex instance

The trainers should have shared with you the URL of a Cortex instance which will allow you to test additional subscription-based and commercial analyzers such as DomainTools, CIRCL pSSL and pDNS, PhishTank, etc.

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:

```
# 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-NSEC" {
    # URL of the Cortex server.
    url = "http://URL_SHARED_BY_THE_TRAINERS_GOES_HERE"
    key ="DJp9GxRaen1YF3wxaTTFY1ewdgnp1zg7"
  }
```

```
      }
```

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.

Step 7 – Configure the MISP Search and the MISP Warning Lists Analyzers

Go to https://github.com/TheHive-Project/CortexDocs and look for the documentation that will show you how to configure the MISP Search and MISP Warning Lists analyzers.

Step 8 – Copy the case study data

The trainers will circulate USB keys. Copy the following files from them to your computer:

```
      doc_file_abbe6618d1ea53a9605b22b44c1ee803.zip
      suspicious-email-observables.txt
```

Please note that the ZIP file is a password-protected archive. The password will be shared during the training.