SECURITY WORKSHOP: THREAT INTEL SHARING WITH MISP

LIVIU VÂLSAN

SPRING 2017 HEPIX, BUDAPEST

WHAT WILL YOU GET OUT OF THIS WORKSHOP?

- Quick introduction to threat intelligence sharing and MISP (~20 min)
- You will learn (hands-on, ~100 min):
  - How to deploy MISP automatically using Puppet
  - How to configure MISP
  - How to create Indicators of Compromise (IoCs)
  - How to share information
  - How to make use of the threat intel (make it actionable)
- You will receive access to the central WLCG MISP instance

WHY SHARE INDICATOR OF COMPROMISE?

- For **detection** purposes
  - Do I have infected systems in my infrastructure?

- For **blocking** purposes
  - I use these attributes to block, sinkhole or divert traffic.

- For **performing intelligence**
  - Gathering information about campaigns and attacks. Are they related? Who is targeting me? Who are the adversaries?

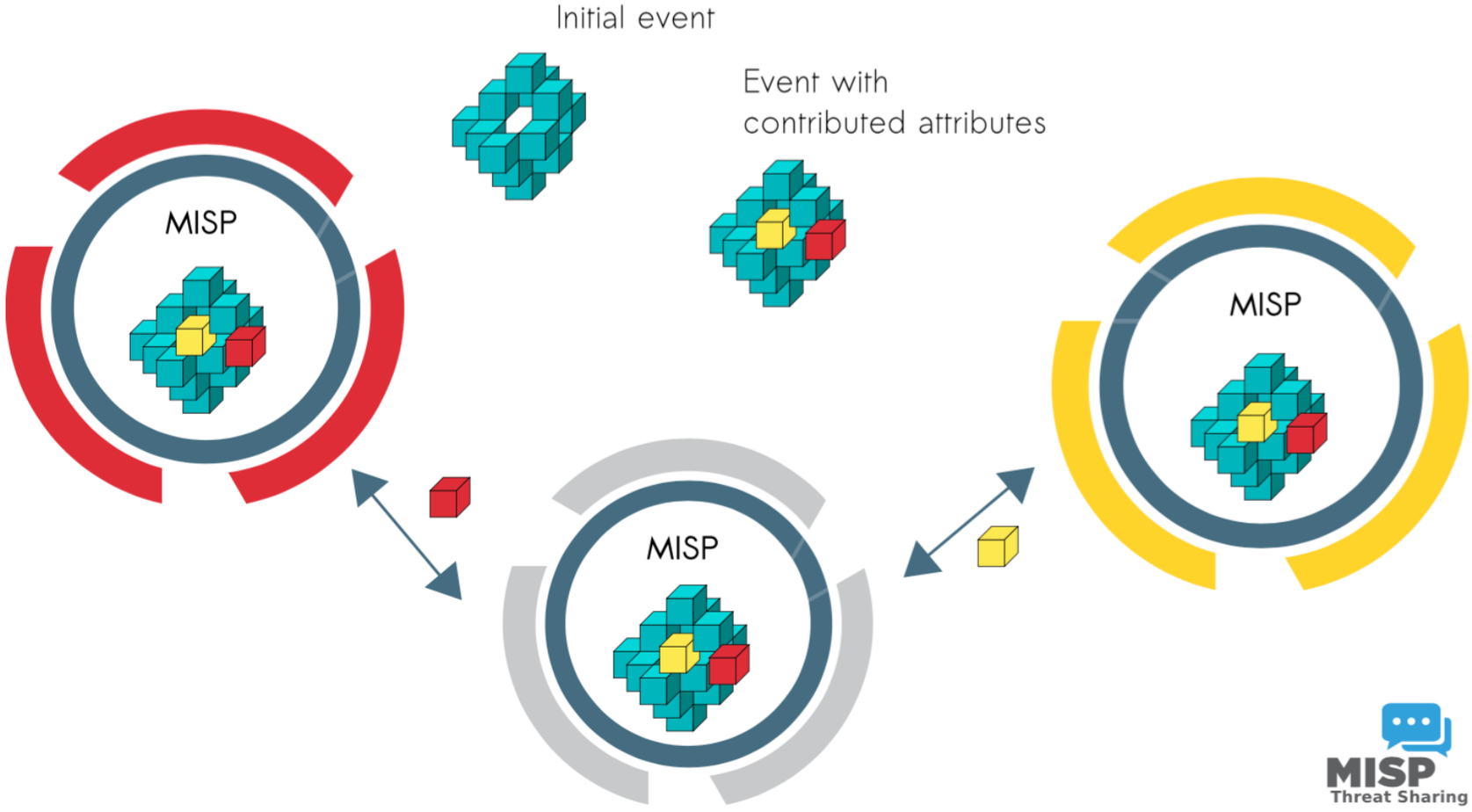
- These objectives can be conflicting (e.g. false-positives have different impacts)

WHAT'S MISP?

- MISP is an open source project for sharing Indicators of Compromise (IoCs)
  - Project homepage: http://www.misp-project.org
  - GitHub repository: https://github.com/MISP/MISP
- Core developers from CIRCL (Computer Incident Response Center Luxembourg) with contributions from many other organizations:
  - Belgian Ministry of Defence (CERT), NATO NCIRC, CERT-EU, CERN, Airbus, ...
- Development based on user feedback
- Very active project

MISP CORE FUNCTIONALITY

- MISP's core functionality is that of sharing threat intelligence, 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.



MISP FEATURES

- MISP has many functionalities:
  - Flexible sharing groups, automatic correlation, free-text import helper, event distribution and collaboration, …
- Many export formats supporting:
  - IDSes / IPSes: Bro, Snort, Suricata, …
  - SIEMs: CEF, …
  - Host scanners: OpenIOC, STIX, CSV, Yara, …
  - Analysis tools: Maltego, …
  - DNS policies: RPZ, …

MISP ATTRIBUTES

- Attributes are Indicators of Compromise and more:
  - They contain a pattern that can be used to detect suspicious or malicious activity: the value of the attribute
  - A type: IP, MD5, URL, domain, etc.
  - An attribute is always in a category (e.g. payload delivery) which tells a story and a context.
  - Can be network indicators (e.g. IP address), system indicators (e.g. a string in memory) or even bank account details
  - An IDS flag on an attribute allows to determine if an attribute can be automatically used for detection.

MISP EVENTS

- Events:
  - A container for grouping attributes related to a given security event (an incident, a malware variant, a campaign, etc)

INSTALLING MISP

- Login on the MISP training VM as root
  - From a Unix based system:

    ```
    ssh -p 2222 root@localhost
    ```

  - The root password is (without the double quotes):

    ```
    “centos”
    ```

INSTALLING MISP

- Fetch the required Puppet modules by running the following commands (the second command may take a while to complete):

```
cd /etc/puppet/modules/
./fetch_puppet_modules.sh
```

- Fetch the main MISP Puppet module by running:

```
puppet module install puppet-misp
```

INSTALLING MISP

- The MISP Puppet module is configuring MISP to run on port 443. Given the limitations of the network setup at HEPiX and the need for port forwarding, MISP will need to run on port 8443. Edit the `/etc/puppet/modules/misp/templates/config.php.erb` file and on line 21 replace `'baseurl' => 'https://<%= @fqdn -%>',` by `'baseurl' => 'https://<%= @fqdn -%>:8443',`
- You can do this change by running the following command (copy & paste it in the terminal):

```
sed -i "s/'baseurl' => 'https:\/\/<%= @fqdn -%>',/'baseurl' => 'https:\/\/<%= @fqdn -%>:8443',/" /etc/puppet/modules/misp/templates/config.php.erb
```

INSTALLING MISP

- The MISP Puppet module is using the FQDN of the host as the base URL for MISP (see previous slide for details).
- To ensure that URLs are correct after MISP is configured set the hostname to your IP address on the WiFi network. This is the same IP that you used for the “MISP HTTPS” rule in the setup instructions.
- Replace `localhost.localdomain` in `/etc/hostname` with the IP address of your laptop on the WiFi network (the IP address will have the format 172.16.x.y).
- In addition run the following command:

  `hostname <ip_address>`

INSTALLING AND CONFIGURING MISP

- Now it's time to install and configure MISP. Run the following command to apply the Puppet manifest:

  ```
  puppet apply /etc/puppet/manifests/site.pp
  ```

- Please not that the above command may take up to 15-20 minutes to complete. Except for 3 errors at the beginning (due to Puppet running masterless) there should be no other errors in applying the manifest. However, due to intermittent network connectivity issues, in case any errors are reported try to rerun the `puppet apply` command.
- Since we want to ensure that all services needed by MISP are available at boot time run the following command to apply the Puppet manifest when the VM boots:

  ```
  echo "puppet apply /etc/puppet/manifests/
  site.pp" >> /etc/rc.local
  ```

IMPORT THE DATABASE SCHEMA

- Run the following command to do the initial import of the database schema:

  ```
  mysql -u misp -p misp < /var/www/MISP/
  INSTALL/MYSQL.sql
  ```

- The password for connecting to the database is (without the double quotes): “`mispdb`”

LOGGING IN TO MISP FOR THE FIRST TIME

- Congratulations, at this point you should have a fully installed and configured MISP instance.
- It's now time to log into MISP for the first time.
- Access the following URL in a browser on your host (laptop): https://<ip_address>:8443. Here again, <ip_address> is your IP on the WiFi network.
- Since this test MISP deployment is using a self signed SSL certificate you will be prompted by a certificate warning, that's normal.
- Once the warning acknowledged you should be prompted by the MISP login page.
- The default username is "`admin@admin.test`" and the default password is "`admin`". You will be required to change the password at the first login.

CREATING INTELLIGENCE

- It's now time to create your first security event.
- From the "Event Actions" menu click on "Add Event"
- Enter some event details in the "Event Info" textbox. This will be used as the event title.
- Click the "Add" button.
- At this point you created a security event, but without any attributes (IoCs)
- For an event to be useful it needs to contain one or usually more attributes (IoCs)
- Scroll down and press the small "+" button located just above the header for the "Date" column
- Choose a category, a type and input a value for the attribute. The "for Intrusion Detection System" checkbox should be checked if the attribute should be used for detection.

SYNCHRONIZING BETWEEN DIFFERENT INSTANCES (1)

- Now that you have a first event created it's time to set up synchronizations with other instances.
- First go to the "Administration" menu and click on "List Organisations"
- Click the edit button (left most button under the "Actions" column) and enter the following UUID: "58fe6b1a-b400-4eea-a997-30210a00020f". This is to ensure that the various "HEPiX" MISP organizations across the different instances share the same UUID.

SYNCHRONIZING BETWEEN DIFFERENT INSTANCES (2)

- We will now setup a dedicated sync user
- From the “Administration” menu click on “Add User”
- Enter an email address, leave the “Set password” checkbox unchecked, choose “HEPiX” as the organization, change the role to “Sync user” and make sure that the following checkboxes at the bottom of the page are unchecked: “Receive alerts when events are published”, “Receive alerts from "contact reporter" requests”, “Send credentials automatically”
- Finally click on the “Submit” button
- You should now receive a confirmation of the new user being added and should get redirected to a table of existing users (there should be one admin and one sync user)
- You will need to provide the hash value found under the “Authkey” column for the sync user to other people you want to peer with

HOW TO ADD A SYNCHRONISATION SERVER

- By now hopefully you've found another workshop participant with a fully deployed MISP instance and you have received an Authkey from them (given the size of the Authkey it's recommended that it's copy&pasted to avoid any typing mistakes).
- Go to the "Sync Actions" menu and click on "List Servers".
- Click on "New Server" from the left hand menu.
- For the base URL use `https://<ip_address>:8443` where `<ip_address>` is the WiFi address of the other person with which you want to set up a peering.
- Enter a label identifying that other MISP instance under the "Instance name" field.
- Enter the Authkey you received from the other person under the "Authkey" field
- Make sure to check the "Push", "Pull" and "Self Signed" checkboxes.
- You should now be redirected to a table showing the remote server.

PULLING FROM / PUSHING TO REMOTE SERVERS

- You have a set of buttons for pushing and pulling under the “Actions” column. The magnifying glass button will allow you to browse the events on the remote instance.
- Try to press the “Push all” button (arrow pointing up), wait 30 seconds and then browse the events on the remote MISP instance.
- What did happen? Can you find your event on the remote instance? If not, why not?

PUBLISHING EVENTS

- Events will not get synchronized unless they are published. Since we just created our event, but never published it, it's normal that it didn't reach the remote MISP instance.
- View your event and click on the "Publish (no email)" option from the left hand side menu.
- The event status will now change to published.
- Go back to the list of sync servers and try to do a push again. What happened this time? Was the event synchronized on the remote server?
- At this point you can also try to pull events from the remote MISP instance.

MAKING INTELLIGENCE ACTIONABLE

- At this point let's see how we can make the intelligence actionable. Let Liviu know your IP address and the value of the Authkey for your local sync user.
- He will then add your instance to a script that runs every 5 minutes, exporting your IoCs to the Bro Intrusion Detection System.
- For your IoCs to be actionable they need to have the "for IDS" flag set.
- By simulating user activity on a monitored VM he will demonstrate how the threat intel you added can be used for detection of malicious activity.

CONTRIBUTING TO EXISTING EVENTS

- Besides being able to produce and consume events, one can also contribute to existing events by proposing either new attributes or changes to existing attributes which are part of an event created by someone else.
- Open an event that you received from a remote instance. The left most button in the “Actions” column allows you to propose edits to existing attributes. A link on the left hand menu “Propose Attribute” allows you to propose new attributes. Try to make some proposals and then push again to the remote instance. Check with the people you sync with, what will they get on their side?

FREETEXT IMPORT IN MISP

- Manually adding intel into MISP can get tedious. Luckily MISP is able to ingest information through a multitude of different means.
- One MISP feature is that of performing a freetext import. Find a public security report focusing on one malware family, exploit or data leak.
- Create a new MISP event for it.
- Click on “Populate from…” on the left hand menu.
- Choose “Freetext import” and copy & paste in the textbook the contents of the public report. What was the outcome of this operation?

OTHER STEPS

- Experiment with setting different distribution settings for the various events you create. How does that impact the synchronization? Check how the distribution is set on remote MISP instances.
- Find some other instances that are connected to instances that you are directly connected to. How do your events propagate to those instances?
- Don’t forget to ask Liviu for access to the central WLCG MISP instance

BACKUP SLIDES

SETTING UP MISP WITH PUPPET

- The MISP Puppet module is very comprehensive and can cover almost all configuration options for MISP. For more details please see the documentation at: https://github.com/voxpupuli/puppet-misp

MORE DOCUMENTATION

- Official MISP training materials:
  - https://www.circl.lu/services/misp-training-materials/
- Official MISP documentation:
  - HTML: https://www.circl.lu/doc/misp/
  - PDF: https://www.circl.lu/doc/misp/book.pdf
- More details on the project's website:
  - http://www.misp-project.org/documentation/