



MISP(THREAT SHARING)

THREAT INTELLIGENCE WITH MISP

MISP PROJECT REPORT

Contents

1	Intro to MISP	3
1.1	Key Features and Capabilities	3
2	Basics of MISP	4
3	CHEATSHEET FOR MISP	5
4	Setting Up MISP	6
4.1	System Requirements	6
4.2	Installation Steps	6
4.3	Configure Network Settings	9
4.4	Access MISP directly from the MISP VM	15
4.4.1	Step 1: Install a Lightweight Desktop Environment	15
4.4.2	Step 2: Install a Display Manager	16
4.4.3	Step 3: Install Firefox	17
4.4.4	Step 4: Start the GUI	17
5	EVENT CREATION	19
5.1	What is an Event	19
5.2	First, to add an Event in MISP, go to Event Actions + Add Event:	19
5.3	Next, fill out the metadata about the Event:	20
5.4	Adding Tags	21
5.5	Adding Galaxy Clusters	21
6	Populating an Event	23
6.1	Adding MISP Attributes	23
6.2	Automated Data Upload	24
7	Creating Multiple Users and allowing them to communicate on a shared malware	26
8	Decaying Model Tools	27
8.1	Step 1: Understanding Decaying Models	27
8.2	Step 2: Available Decaying Tools	27
8.3	Step 3: Configuring Decay in MISP	27
9	Steps to Generate API Key for Automation and Integration	30
10	Automation for Advanced Threat Detection and Intelligence Module	31
10.1	Fetch Threat Feeds from OSINT Sources	31
11	Steps to Integrate AlienVault OTX with MISP	31
11.1	Prerequisites	31
11.2	Configuring MISP to Fetch Data from OTX	31
12	Installing MISP Modules	33
12.1	Step 1: Install MISP Modules	33
12.2	Step 2: Install System Dependencies	33
12.3	Step 3: Install Additional Python Packages	33
12.4	Step 4: Run MISP Modules	33

12.5 Step 4: Run MISP Modules	34
13 Enriching Events with VirusTotal	34
13.1 Step 1: Enable the VirusTotal Module	34
13.2 Step 2: Configure API Key	35
13.3 Step 3: Enrich an Event Using VirusTotal	35
13.4 Step 4: Review and Utilize the Enriched Data	36
14 Correlate Threat Feeds with Vulnerabilities	38
14.1 Prerequisites for performing Correlation	38
15 ELK Stack for Threat Intelligence Correlation	40
15.1 Installing ELK Stack	41
15.1.1 Step 1: Install Elasticsearch	41
15.1.2 Step 2: Install Logstash	41
15.1.3 Step 3: Install Kibana	41
15.2 how ELASTICSEARCH works for correlation	42
15.3 Creating data views	45
15.4 Performing correlation between cves of misp and nvd	47
16 Correlation Queries in Kibana Console	48
16.1 Retrieving Data from MISP and NVD Indices	48
16.2 Extracting CVE Names from MISP	49
16.3 Filtering NVD Data for a Specific CVE	50
16.3.1 Conclusion	51
17 correlation without ELK	52
18 Detailed Project Repository without using elk	57

1 Intro to MISP



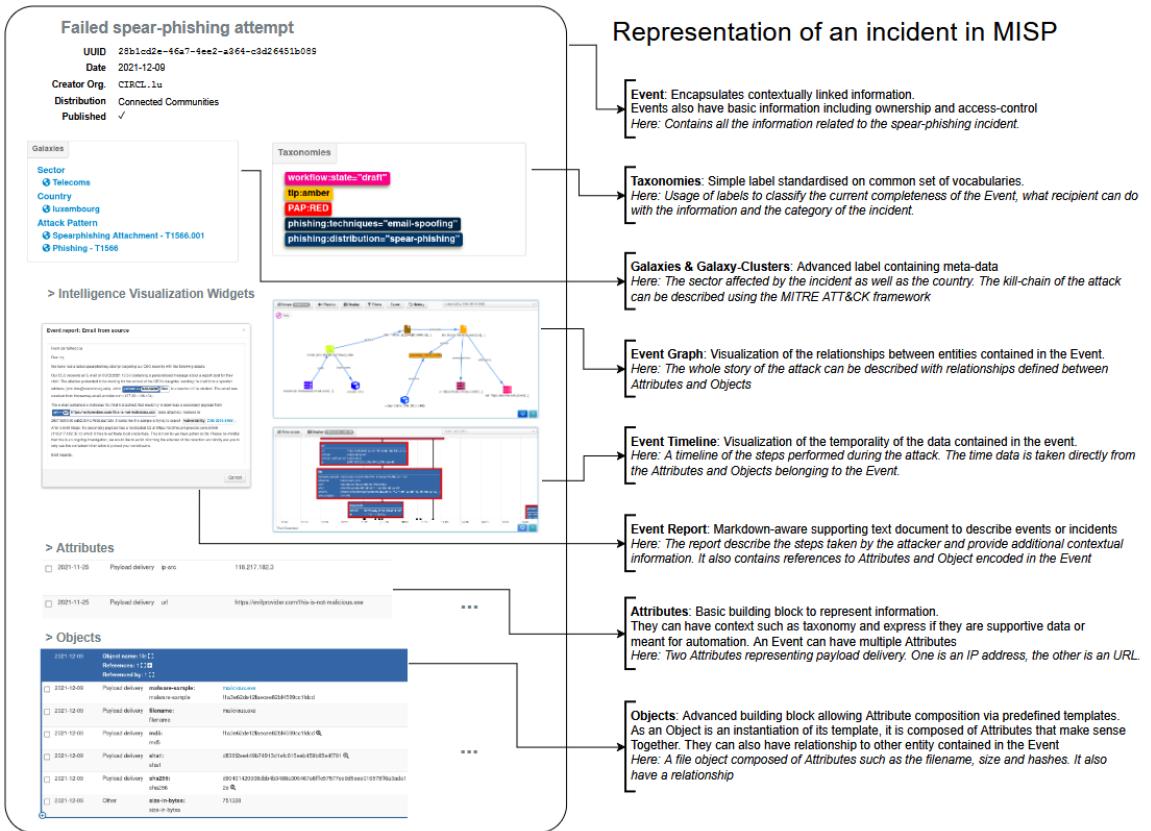
MISP (Malware Information Sharing Platform and Threat Sharing) is an open-source threat intelligence platform that allows you to share, collate, analyze, and distribute threat intelligence.

1.1 Key Features and Capabilities

- **Data Ingestion:** Import and aggregate threat intelligence from various sources
- **Data Structuring:** Organize data using Events, Attributes (IOCs), and Objects
- **Information Sharing:** Share intelligence with trusted partners and communities
- **Taxonomies:** Use standardized classification systems (CAPEC, CVE, MITRE ATT&CK)
- **Data Enrichment:** Add contextual information and threat actor profiles
- **Customization:** Adapt MISP instance to specific organizational needs
- **Integration:** Connect with various security tools and platforms
- **Analysis:** Automatic correlation of threat intelligence patterns
- **Alerting:** Notification system for specific threat events
- **API Access:** RESTful API for programmatic integration

2 Basics of MISP

The platform provides a structured and standardized framework for collecting, storing, and sharing threat intelligence data, enabling collaboration and enhanced defense against cyber threats. It has mappings with existing threat intelligence frameworks (e.g., MITRE ATTCK, CAPEC, etc.) and strong integrations with security products (e.g., CrowdStrike Falcon, Intel471, etc.). MISP is the defacto open-source threat intelligence platform mature organizations use to track threats and collaborate.



3 CHEATSHEET FOR MISP

MISP Data Model Cheat Sheet

- ❖ Context such as Taxonomies or Galaxy Clusters can be attached to the element
- ❖ Has a distribution level
- ❖ Can be synchronised to/from other instances

Event

Encapsulations for contextually linked information.

Purpose: Group datapoints and context together. Acting as an envelop, it allows setting distribution and sharing rules for itself and its children.
Usecase: Encode incidents/events/reports/...
► Events can contain other elements such as Attributes , MISP Objects and Event Reports .
► The distribution level and any context added on an Event (such as Taxonomies) are propagated to its underlying data.

Attribute

Basic building block to share information.

Purpose: Individual data point. Can be an indicator or supporting data.
Usecase: Domain, IP, link, sha1, attachment, ...
► Attributes cannot be duplicated inside the same Event and can have Sightings .
► The difference between an indicator or supporting data is usually indicated by the state of the attribute's to_ids flag.

MISP Object

Advanced building block providing Attribute compositions via templates.

Purpose: Groups Attributes that are intrinsically linked together.
Usecase: File, person, credit-card, x509, device, ...
► MISP Objects have their attribute compositions described in their respective template. They are instantiated with Attributes and can Reference other Attributes or MISP Objects .
► MISP is not required to know the template to save and display the object. However, edits will not be possible as the template to validate against is unknown.

Object Reference

Relationships between individual building blocks.

Purpose: Allows to create relationships between entities, thus creating a graph where they are the edges and entities are the nodes.
Usecase: Represent behaviours, similarities, affiliation, ...
► References can have a textual relationship which can come from MISP or be set freely.

Sightings

Means to convey that an Attribute has been seen.

Purpose: Allows to add temporality to the data.
Usecase: Record activity or occurrence, perform IoC expiration, ...
► Sightings are the best way to express that something has been seen. They can also be used to mark false positives.

Event Report

Advanced building block containing formatted text.

Purpose: Supporting data point to describe events or processes.
Usecase: Encode reports, provide more information about the Event , ...
► Event Reports are markdown-aware and include a special syntax to reference data points or context.

Proposals

Clone of an Attribute containing information about modification to be done.

Purpose: Allow the correction or the creation of Attributes for Events your organisation does not own.
Usecase: Disable the IDS flag, Correct errors
► As Proposals are sync., if the creator organisation is connected to the MISP instance from where the Proposal has been created, it will be able to either accept or discard it.

Taxonomies

Machine and human-readable labels standardised on a common set of vocabularies.

Purpose: Enable efficient classification globally understood, easing consumption and automation.
Usecase: Provide classification such as: TLP, Confidence, Source, Workflows, Event type, ...
► Even though MISP allows the creation of free-text tags, it's always preferable to use those coming from Taxonomies , if they exist.

Galaxies

Act as a container to group together context described in Galaxy Clusters by their type.

Purpose: Bundle Galaxy Clusters by their type to avoid confusion and to ease searches.
Usecase: Bundle types: Exploit-Kit, Preventive Measures, ATT&CK, Tools, Threat-actors, ...

Galaxy Clusters

Knowledge base items used as tags with additional complex meta-data aimed for human consumption.

Purpose: Enable description of complex high-level information for classification.
Usecase: Extensively describe elements such as: threat actors, countries, technique used, ...
► Galaxy Clusters can be seen as an enhanced Taxonomy as they can have meta-data and relationships with other Galaxy Clusters .
► Any Galaxy Clusters can contain the following:

- Cluster Elements: Key-Value pair forming the meta-data.

Example: Country:LU, Synonym:APT28,
 Currency:Dollar, refs:https://*,
 ...

- Cluster Relations (🔗): Enable the creation of relationships between one or more Galaxy Clusters .

Example: Threat actor X is similar to threat actor Y with high-likelihood.

4 Setting Up MISP

MISP (Malware Information Sharing Platform) is an open-source threat intelligence platform that enables security professionals to collect, share, and correlate threat data efficiently. This section outlines the step-by-step process to install and configure MISP.

4.1 System Requirements

Before installing MISP, ensure that your system meets the following requirements:

- Ubuntu 24.04 or a compatible Linux distribution
- At least 4GB RAM (8GB recommended for production)
- Minimum 2 CPU cores
- 20GB of disk space (more for large-scale deployments)

4.2 Installation Steps

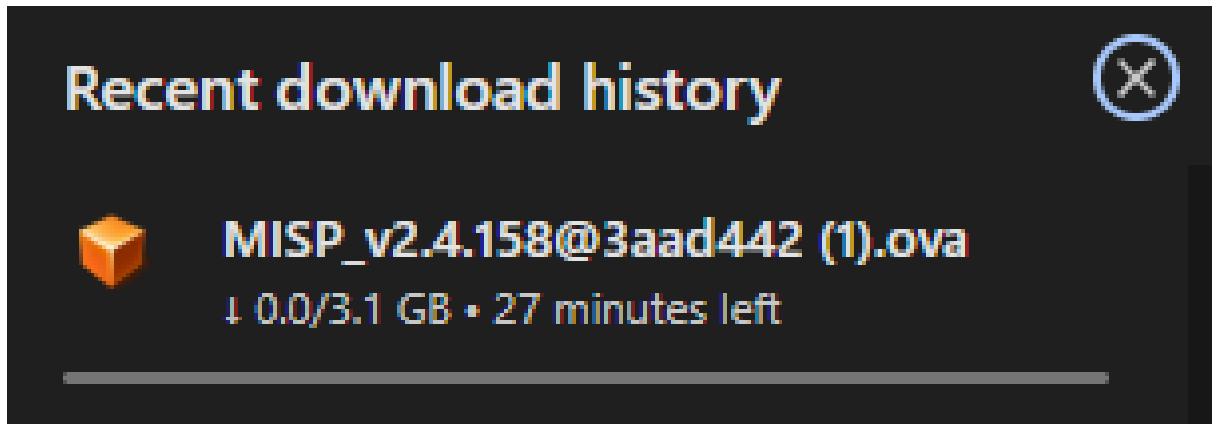
To install MISP, follow these steps:

1. So, we will start first downloading MISP virtual machine(OVA) from this link:-

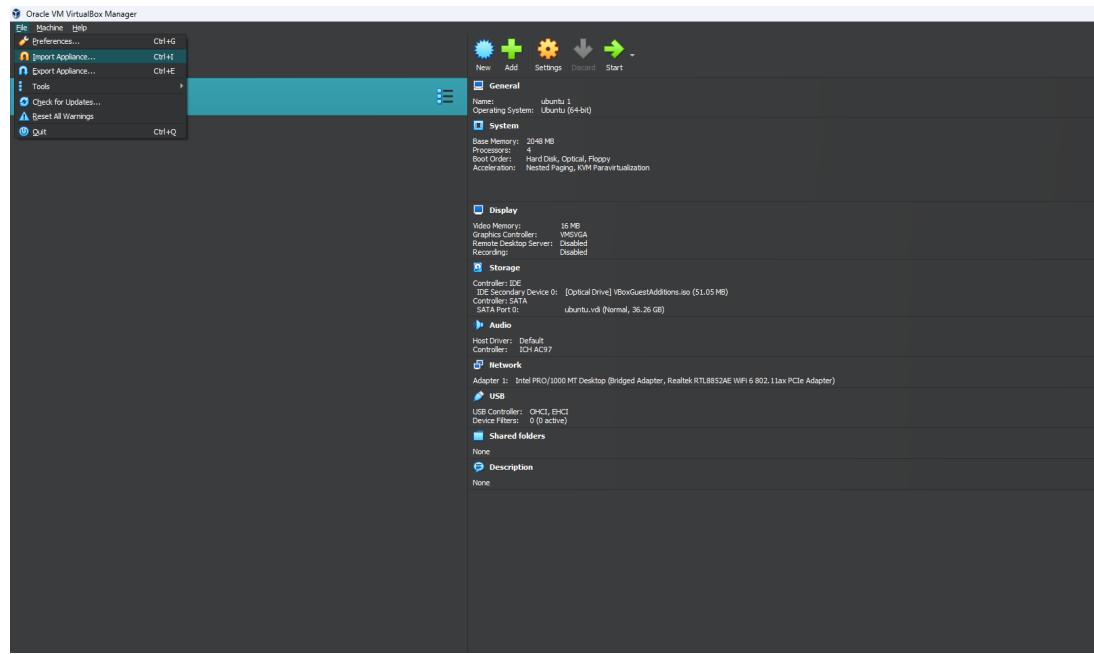
https://vm.misp-project.org/latest/MISP_v2.4.158@3aad442.ova

Once you click the above link ,this will directly start the downloading of MISP VM(virtual machine)

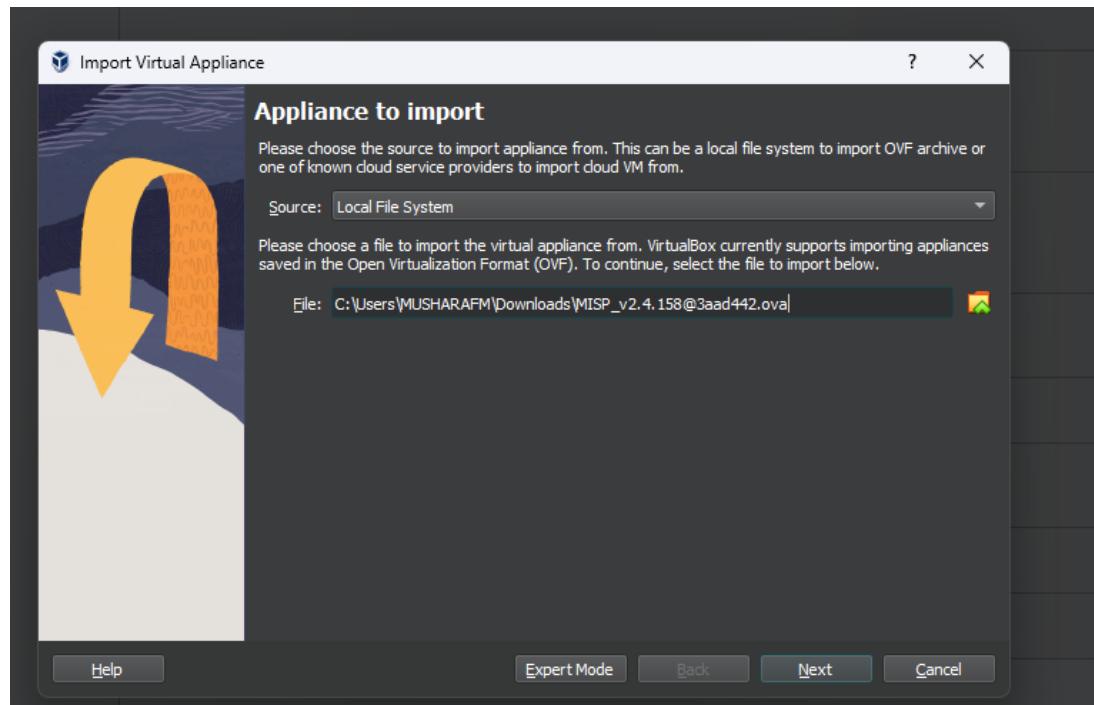
In your downloads sections you will see something like this



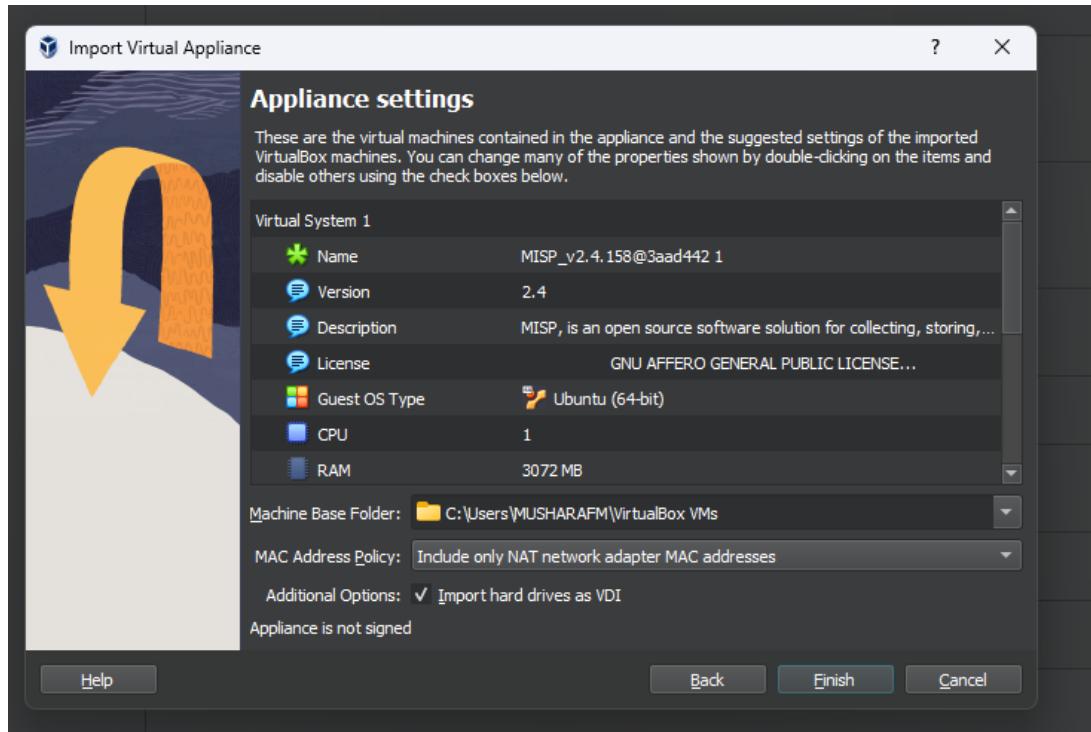
2. After downloading the machine locally we head over to our virtual box. Open Oracle VM VirtualBox.
 - Go to File → Import Appliance.



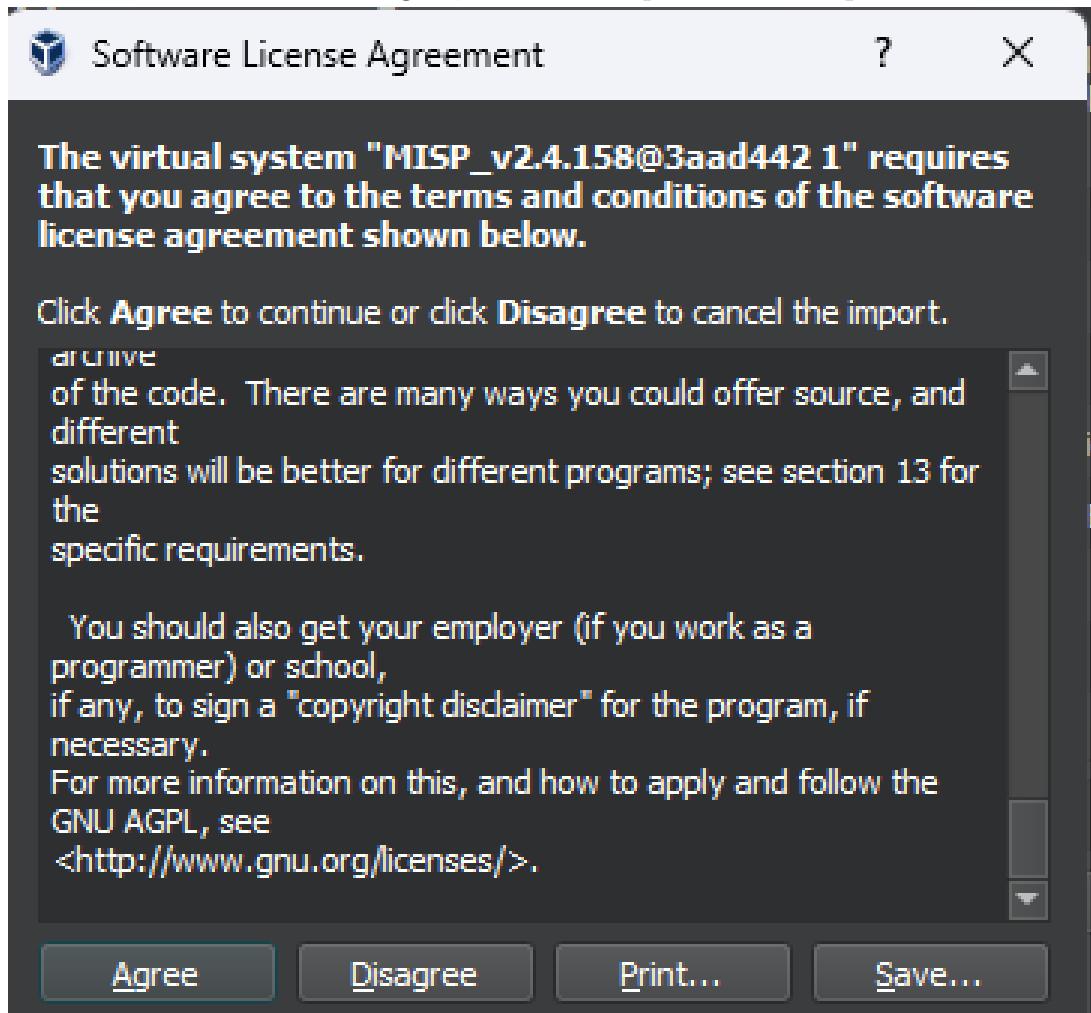
- once you click Import Appliance, you will see this interface, here press next.



- Click Next, then review the VM settings (CPU, RAM, Disk).



- Click finish and then click Agree, wait for the process to complete.

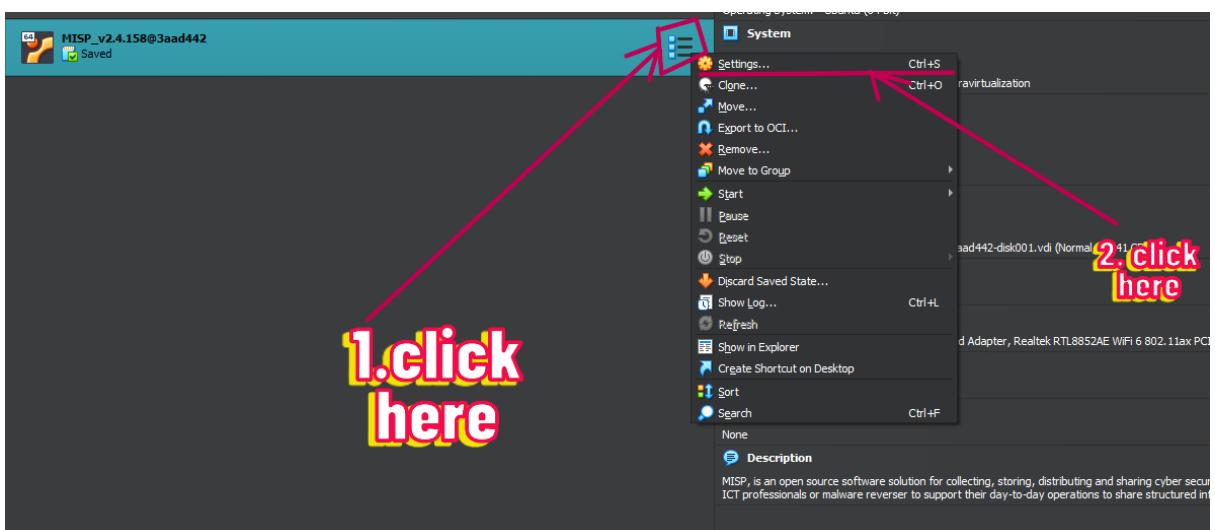


once you are done with the above steps your machine will be ready like this.

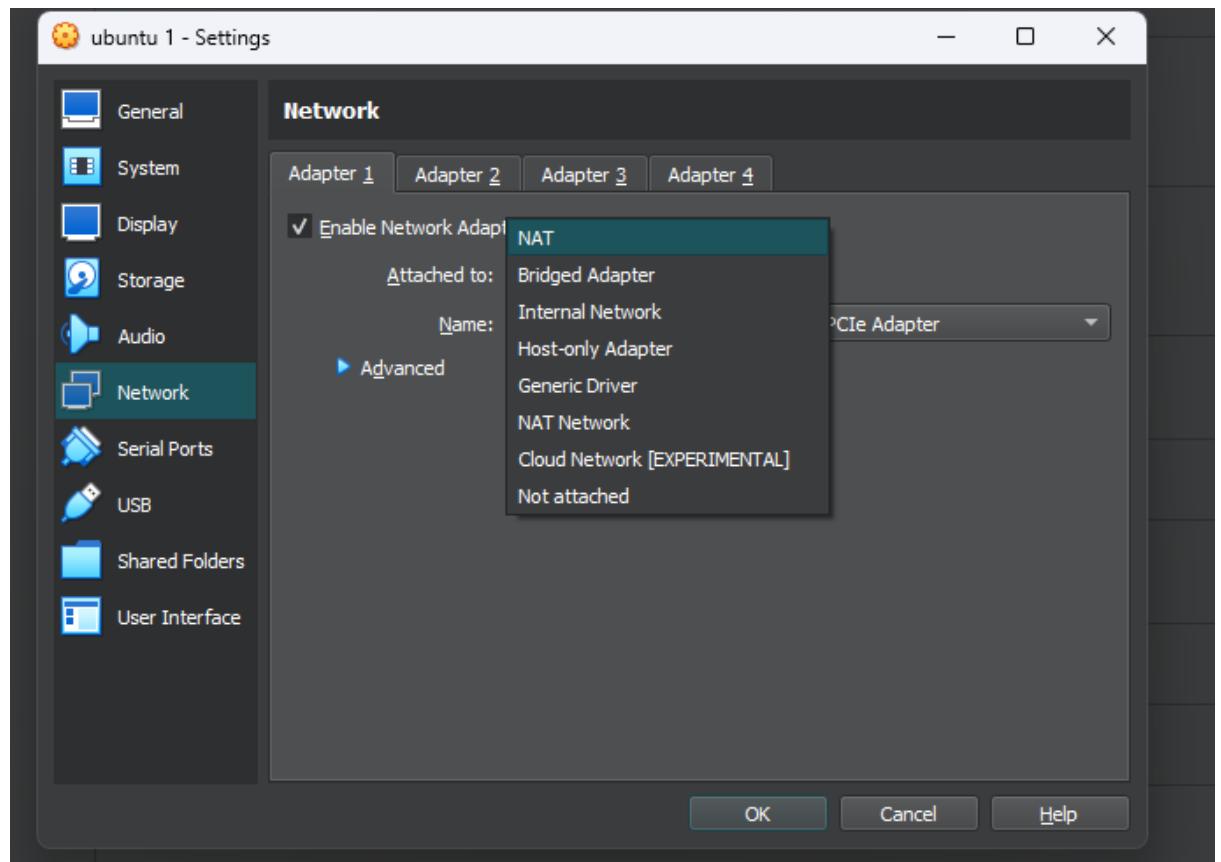


4.3 Configure Network Settings

After installation, configure MISP by setting up the following:

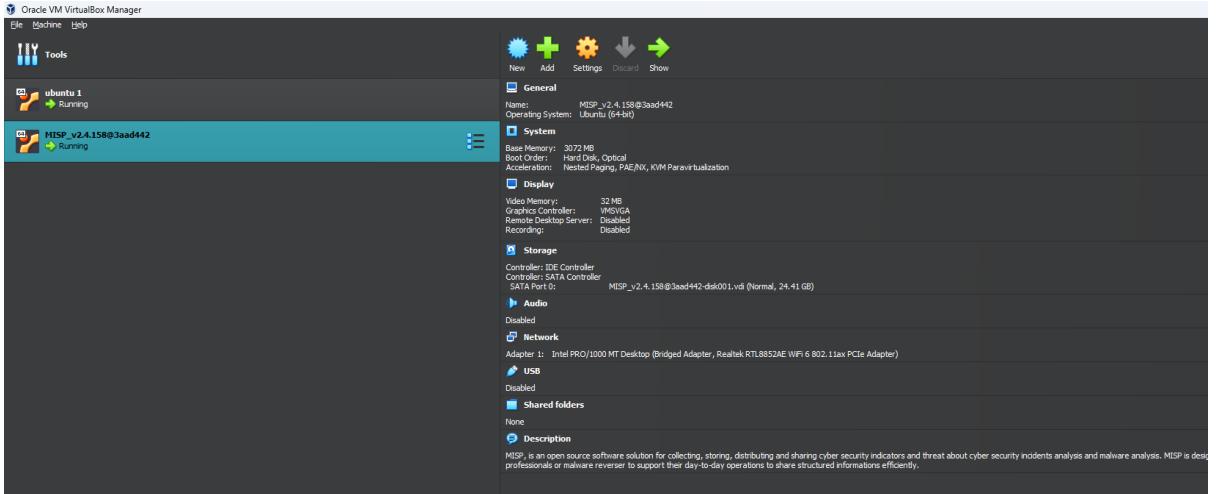


- Go to Settings → Network and choose:
- Bridged Adapter (if you want it on the same network as your host).
- NAT (if you just need internet access).



note: when using a bridged adapter you will be able to access misp locally on your already preinstalled Ubuntu and use NAT if you want to access misp dashboard on MISP VM.

Ok so now you might be confused here why I asked you to have pre-installed Ubuntu with misp VM, you will get the answer in next 2 parts. That is 2 virtual machines in the virtual box like this, one Ubuntu and one misp VM.



part 1:

- Now, once you have got all this setup, you will go to Settings → Network and choose Bridged Adapter for both machines.
- And once you start the MISP VM, You will see the interface like this.

```
Welcome to the MISP Threat Sharing VM.
---

IP address: 172.31.102.176

---

MISP      http://172.31.102.176      admin@admin.test / admin
          https://172.31.102.176
MISP-modules (API) http://172.31.102.176:6666 (no credentials)
MISP-dashboard   http://172.31.102.176:8001 (no credentials)
Viper-web       http://172.31.102.176:8888 admin / Password1234
jupyter-notebook http://172.31.102.176:8889

The default system credentials are: misp / Password1234

On VirtualBox port-forwarding from your host to the guest is in place.
Below are the forwards as we need to use ports >1024 for some.

MISP      -> 8080 and :8443
ssh      -> 2222
misp-modules -> 1666

If this fails, make sure the host machine is not occupying one of the forwarded ports or a firewall is active.

misp login: misp
Password:
Last login: Fri May 13 15:04:13 CEST 2022 from 192.168.151.1 on pts/0
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-177-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
misp@misp:~$ time
Traceback (most recent call last):
  File "/usr/lib/command-not-found", line 27, in <module>
    from CommandNotFound.util import crash_guard
ModuleNotFoundError: No module named 'CommandNotFound'
misp@misp:~$ time

real    0m0.000s
user    0m0.000s
sys     0m0.000s
misp@misp:~$ date
Wed Jan 29 08:18:19 CET 2025
misp@misp:~$
```

here you will have to login first with the following credentials as shown in dashboard

- MISP login →MISP
- MISP password →Password1234

- (d) once you are logged in successfully, you can take the IP address of MISP dashboard and the put it in your browser inside your UBUNTU.

```
Welcome to the MISP Threat Sharing UM.
---
IP address: 172.31.102.176
---
MISP      http://172.31.102.176      admin@admin.test / admin
MISP-modules (API) https://172.31.102.176:443 (no credentials)
MISP-dashboard http://172.31.102.176:8001 (no credentials)
Viper-web    http://172.31.102.176:8888 admin / Password1234
jupyter-notebook http://172.31.102.176:8889

The default system credentials are: misp / Password1234

On VirtualBox port-forwarding from your host to the guest is in place.
Below are the forwards as we need to use ports >1024 for some.

MISP      -> 8080 and :8443
ssh       -> 2222
misp-modules -> 1666

If this fails, make sure the host machine is not occupying one of the forwarded ports or a firewall is active.

misp login: misp
Password:
Last login: Fri May 13 15:04:13 CEST 2022 from 192.168.151.1 on pts/0
Welcome to Ubuntu 18.04.6 LTS (GNU/Linux 4.15.0-177-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:   https://landscape.canonical.com
 * Support:      https://ubuntu.com/advantage
misp@misp:~$ time
Traceback (most recent call last):
  File "/usr/lib/command-not-found", line 27, in <module>
    from CommandNotFound.util import crash_guard
ModuleNotFoundError: No module named 'CommandNotFound'
misp@misp:~$ time

real    0m0.000s
user    0m0.000s
sys     0m0.000s
misp@misp:~$ date
Wed Jan 29 08:18:19 CET 2025
misp@misp:~$
```

**put this IP in
your Ununtu's
browser**

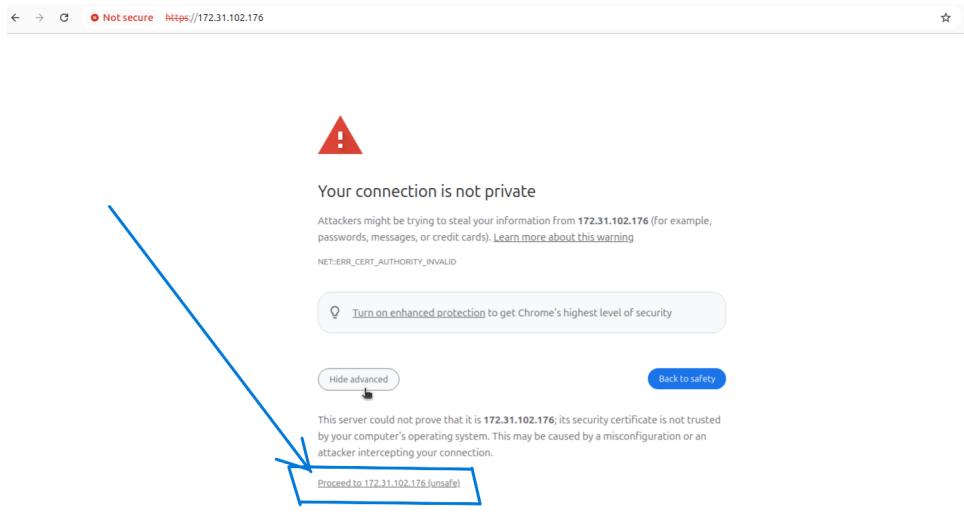
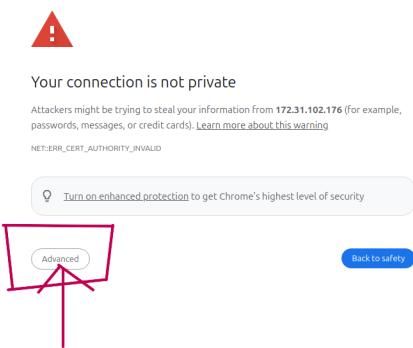
**Use these
credentials
for login**

**here you'll have
to put misp login
credentials.**

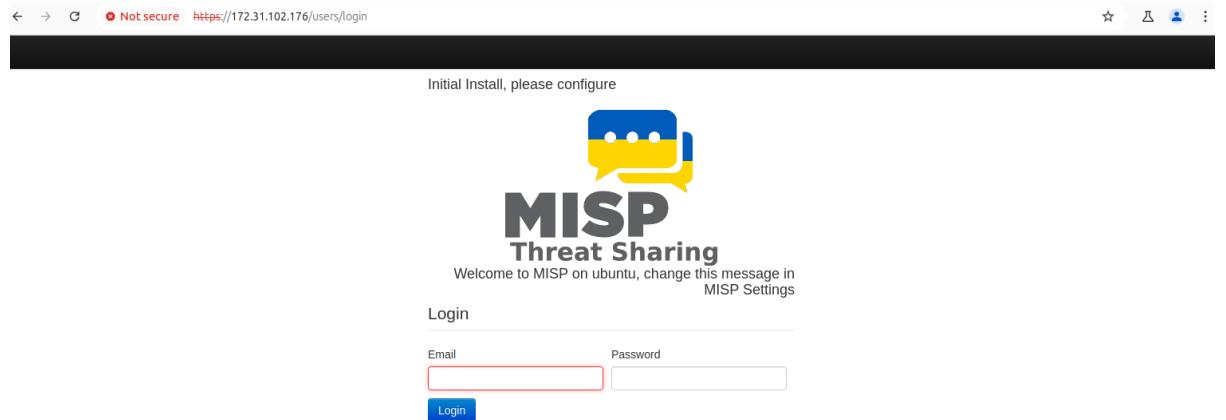
**you will see
this after
you're logged
in
successfully**

- (e) After obtaining the IP address of the MISP dashboard, open Firefox or any other browser in Ubuntu and enter the MISP dashboard IP in the browser's address bar. This will allow you to access the MISP web interface.

← → ⌛ ⓘ Not secure https://172.31.102.176 ☆ 🔍 🌐 ⚙



once you click **proceed to ip-address** you will see the MISP dashboard Interface:



here you can enter misp default login credentials as **email → admin@admin.test** and **password → admin**

part 2:

- (a) Now, the question arises why not access misp dashboard in the misp VM itself?
- (b) While this is possible, the MISP VM runs on a minimal Ubuntu/Debian-based system without a graphical user interface (GUI) by default. This means it lacks a web browser like Firefox to access the MISP dashboard.
- (c) **To enable direct access within the MISP VM, you would need to:**
 - i. Install a GUI (such as XFCE or LXDE).
 - ii. Install a display manager (such as LightDM).
 - iii. Install Firefox to browse the MISP dashboard.
- (d) However, the recommended approach is to keep the MISP VM lightweight and dedicated to running MISP, while using a separate Ubuntu VM with a full desktop environment for easier access via a browser.

This setup ensures:

Better performance for MISP, as it remains a dedicated server.

Easier troubleshooting and maintenance.

A familiar browsing experience without additional setup inside the MISP VM.

- (e) That's why we configure two VMs:

- i. MISP VM → Runs the MISP server.
- ii. Ubuntu VM → Accesses the MISP dashboard via Firefox.

OPTIONAL If you still prefer to access MISP directly from the MISP VM, follow the steps to install a GUI and Firefox. However, for most users, using a separate Ubuntu VM is the more practical choice.

4.4 Access MISP directly from the MISP VM

4.4.1 Step 1: Install a Lightweight Desktop Environment

A lightweight desktop environment like XFCE or LXDE is ideal for running a GUI in the MISP VM without consuming excessive resources.

- (a) **Run the following command to install XFCE:**

```
sudo apt update
```

```
misp@misp:~$ sudo apt update
Get:1 http://security.ubuntu.com/ubuntu bionic-security InRelease [102 kB]
Hit:2 http://ppa.launchpad.net/deadsnakes/ppa/ubuntu bionic InRelease
Hit:3 http://ppa.launchpad.net/ondrej/php/ubuntu bionic InRelease
Hit:4 http://us.archive.ubuntu.com/ubuntu bionic InRelease
Get:5 http://us.archive.ubuntu.com/ubuntu bionic-updates InRelease [102 kB]
Get:6 http://us.archive.ubuntu.com/ubuntu bionic-backports InRelease [102 kB]
Fetched 305 kB in 3s (104 kB/s)
Traceback (most recent call last):
  File "/usr/lib/cnf-update-db", line 8, in <module>
    from CommandNotFound.db.creator import DbCreator
ModuleNotFoundError: No module named 'CommandNotFound'
Reading package lists... Done
E: Problem executing scripts APT::Update::Post-Invoke-Success 'if /usr/bin/test -w /var/lib/command-not-found/ -a -e /usr/lib/cnf-update-db; then /usr/lib/cnf-update-db > /dev/null; fi'
E: Sub-process returned an error code
misp@misp:~$
```

```
sudo apt install xfce4 xfce4-goodies -y
```

you should see something like this upon successful execution of the above command:

```
create mode 100644 xdg/autostart/gsettings-data-convert.desktop
create mode 100644 xdg/autostart/pulseaudio.desktop
create mode 100644 xdg/autostart/xfce4-clipman-plugin-autostart.desktop
create mode 100644 xdg/autostart/xfce4-notes-autostart.desktop
create mode 100644 xdg/autostart/xfce4-power-manager.desktop
create mode 100644 xdg/autostart/xfsettingsd.desktop
create mode 100644 xdg/autostart/xscreensaver.desktop
create mode 100644 xdg/menus/xfce-applications.menu
create mode 100644 xdg/menus/xfce-settings-manager.menu
create mode 100644 xdg/tumbler/tumbler.rc
create mode 100644 xdg/xfce4/Xft.xrdb
create mode 100644 xdg/xfce4/helpers.rc
create mode 100644 xdg/xfce4/panel/default.xml
create mode 100644 xdg/xfce4/panel/xfce4-clipman-actions.xml
create mode 100644 xdg/xfce4/whiskermenu/defaults.rc
create mode 100644 xdg/xfce4/xconf/xfce-perchannel-xml/thunar-volman.xml
create mode 100644 xdg/xfce4/xconf/xfce-perchannel-xml/xfce4-keyboard-shortcuts.xml
create mode 100644 xdg/xfce4/xconf/xfce-perchannel-xml/xfce4-power-manager.xml
create mode 100644 xdg/xfce4/xconf/xfce-perchannel-xml/xfce4-session.xml
create mode 100644 xdg/xfce4/xconf/xfce-perchannel-xml/xsettings.xml
create mode 100755 xdg/xfce4/xinitrc
create mode 100644 xfce4/defaults.list
nisp@misp:~$
```

4.4.2 Step 2: Install a Display Manager

- (b) To manage graphical sessions, install LightDM as the display manager:

```
sudo apt install lightdm -y
```

you should see something like this upon successful execution of the above command:

```
create mode 120000 systemd/system/ibus@.service
create mode 120000 systemd/system/dbus-org.bluez.service
create mode 120000 systemd/system/dbus-org.freedesktop.Avahi.service
create mode 120000 systemd/system/dbus-org.freedesktop.ModemManager1.service
create mode 120000 systemd/system/dbus-org.freedesktop.nm-dispatcher.service
create mode 120000 systemd/system/display-manager.service
create mode 120000 systemd/system/multi-user.target.wants/ModemManager.service
create mode 120000 systemd/system/multi-user.target.wants/NetworkManager.service
create mode 120000 systemd/system/multi-user.target.wants/avahi-daemon.service
create mode 120000 systemd/system/multi-user.target.wants/pppd-dns.service
create mode 120000 systemd/system/multi-user.target.wants/wpa_supplicant.service
create mode 120000 systemd/system/network-online.target.wants/NetworkManager-wait-online.service
create mode 120000 systemd/system/sockets.target.wants/avahi-daemon.socket
create mode 100644 usb_modeswitch.conf
create mode 100755 wpa_supplicant/action_wpa.sh
create mode 100755 wpa_supplicant/functions.sh
create mode 100755 wpa_supplicant/ifupdown.sh
create mode 100644 xdg/autostart/gnome-keyring-pkcs11.desktop
create mode 100644 xdg/autostart/gnome-keyring-secrets.desktop
create mode 100644 xdg/autostart/gnome-keyring-ssh.desktop
create mode 100644 xdg/autostart/gnome-screensaver.desktop
create mode 100644 xdg/autostart/indicator-application.desktop
create mode 100644 xdg/autostart/indicator-messages.desktop
create mode 100644 xdg/autostart/nm-applet.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.A11ySettings.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.Clipboard.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.Color.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.Datetime.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.Housekeeping.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.Keyboard.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.MediaKeys.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.Mouse.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.Power.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.PrintNotifications.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.Rfkill.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.ScreenSaverProxy.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.Sharing.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.Smartcard.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.Sound.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.Wacom.desktop
create mode 100644 xdg/autostart/org.gnome.SettingsDaemon.XSettings.desktop
create mode 100644 xdg/autostart/polkit-gnome-authentication-agent-1.desktop
create mode 100644 xdg/autostart/print-applet.desktop
create mode 100644 xdg/autostart/unity-fallback-mount-helper.desktop
create mode 100644 xdg/autostart/unity-settings-daemon.desktop
create mode 100644 xdg/menus/gnome-applications.menu
create mode 100644 xdg/menus/unitycc.menu
nisp@misp:~$
```

4.4.3 Step 3: Install Firefox

- (c) If Firefox is not already installed on your MISP VM, install it using:

```
sudo apt install firefox -y
```

you should see something like this upon successful execution of the above command:

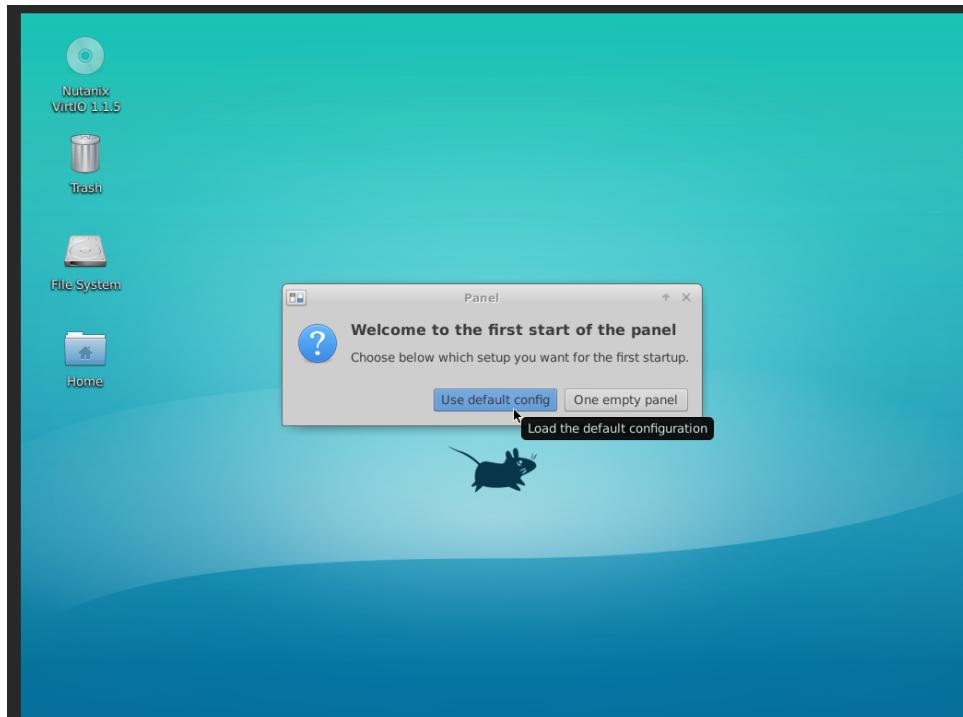
```
create mode 100644 xdg/autostart/gsettings-data-convert.desktop
create mode 100644 xdg/autostart/pulseaudio.desktop
create mode 100644 xdg/autostart/xfce4-clipman-plugin-autostart.desktop
create mode 100644 xdg/autostart/xfce4-notes-autostart.desktop
create mode 100644 xdg/autostart/xfce4-power-manager.desktop
create mode 100644 xdg/autostart/xsettingsd.desktop
create mode 100644 xdg/autostart/xscreensaver.desktop
create mode 100644 xdg/menus/xfce-applications.menu
create mode 100644 xdg/menus/xfce-settings-manager.menu
create mode 100644 xdg/tumbler/tumbler.rc
create mode 100644 xdg/xfce4/Xft.xdb
create mode 100644 xdg/xfce4/helpers.rc
create mode 100644 xdg/xfce4/panel/default.xml
create mode 100644 xdg/xfce4/panel/xfce4-clipman-actions.xml
create mode 100644 xdg/xfce4/whiskermenu/default.rc
create mode 100644 xdg/xfce4/xconf/xfce-perchannel-xml/thunar-volman.xml
create mode 100644 xdg/xfce4/xconf/xfce-perchannel-xml/xfce4-keyboard-shortcuts.xml
create mode 100644 xdg/xfce4/xconf/xfce-perchannel-xml/xfce4-power-manager.xml
create mode 100644 xdg/xfce4/xconf/xfce-perchannel-xml/xfce4-session.xml
create mode 100755 xdg/xfce4/xinitrc
create mode 100644 xfce4/defaults.list
misp@misp:$
```

4.4.4 Step 4: Start the GUI

- (d) After installing the desktop environment, start the GUI manually by running:

```
startx
```

you should see something like this upon successful execution of the above command:



here click **Use default config**

- (e) Once the GUI starts, you should see the XFCE desktop environment. To open Firefox:
- (f) Open the terminal in the GUI and run:

```
firefox
```

So, after following these two methods you will be able to access misp dashboard locally using its IP address.



here, you will use default log in credentials:-

- Email:- admin@admin.test
- password:-admin
- This completes our misp setup

5 EVENT CREATION

5.1 What is an Event

MISP events are “encapsulations for contextually related information represented as attribute and object.” They can be threat intelligence articles, malware analysis reports, threat research, or any other way you can think of representing threat intelligence. Events are the individual containers that group your atomic pieces of threat intelligence with contextual information so analysts can actually use it. They are the main way of interacting with data in MISP.

5.2 First, to add an Event in MISP, go to Event Actions + Add Event:

The screenshot shows the MISP web interface at <https://172.31.102.176/events/index>. The left sidebar has a 'Automation' section with a dropdown menu open, showing options like 'List Events', 'Add Event' (which is highlighted in blue), 'List Attributes', 'Search Attributes', 'View Proposals', 'Events with proposals', 'View delegation requests', 'List Tags', 'List Tag Collections', 'Add Tag', 'List Taxonomies', 'List Templates', 'Add Template', 'Export', and 'Automation'. The main content area displays a list of events. Each event entry includes the organization name, event ID, type, and various attributes. For example, one event is labeled 'Synovus Financial' with ID 983, type 'Attack Pattern', and attributes like 'Phishing - T1566', 'Country:france', and 'Type:OSINT'. Another event is labeled 'ORGNAME ? 1354' with type 'Attack Pattern' and attributes 'Country:france' and 'Type:OSINT'. The bottom of the screen shows the URL <https://172.31.102.176/events/add> and a footer note: 'This is an initial install Powered by MISP 2.4.158. Please configure and harden accordingly - 2025-01-29 12:15:36'.

5.3 Next, fill out the metadata about the Event:

- **Distribution:** How you want your event to be shared across MISP instances (your organization only, this community only, connected communities, or all communities).
- **Threat Level:** The sophistication or danger the threat poses (high, medium, low, or undefined).
- **Analysis:** Which stage of analysis this event is at currently (initial, ongoing, or complete).
- **Event Info:** A title, brief description, or identifier to track the event.
- **Extends Event** If the Event is related to a previous Event, you can link it by the UUID or ID of that previous Event.

You can then click Submit to begin adding data to the Event.

The event could not be saved. Please, try again.

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 2025-01-30	Distribution <small>i</small> Sharing group	Sharing Group CDAC
Threat Level <small>i</small> Medium	Analysis <small>i</small> Ongoing	
Event Info Covert Delivery of Cobalt Strike Beacon via Sophos Phishing Website		
Info cannot be empty.		
Extends Event Event UUID or ID. Leave blank if not applicable.		

Submit

Download: PGP public key This is an initial install Powered by MISP 2.4.158 Please configure and harden accordingly - 2025-01-30 08:26:03

5.4 Adding Tags

The screenshot shows the MISP web interface with the URL <https://172.31.102.176/events/view/1356>. The left sidebar has a 'Tags' icon selected. The main form shows event details like Event ID (1356), UUID (295eadd2-2827-4f67-8172-bec2a41b1502), and Tags (OSINT, tip:white). A 'Tags' input field is highlighted with a blue box.

Next, select the tag you want to add.

5.5 Adding Galaxy Clusters

The screenshot shows the MISP web interface with the URL <https://172.31.102.176/events/view/1356>. The top navigation bar includes links for Pivots, Galaxy, Event graph, Event timeline, Correlation graph, ATT&CK matrix, Event reports, Attributes, and Discussion. The 'Galaxies' tab is selected. Below it, there's a 'Tags' input field with a blue box highlighting it. At the bottom, there are navigation buttons for 'previous' and 'next' and a 'view all' link.

You can attach a MISP galaxy as a cluster to add more context to an Event. Galaxies allow you to describe an Event using shared threat intelligence frameworks or standardized lingo. For instance, you can add the name of malware seen in an Event, map the Event to MITRE ATTCK technique, or add a threat actor.

1356: Covert Deliver...

Add new cluster

Galaxies

mitre-attack

All clusters & Attack Pattern Course of Action Intrusion Set Malware Tool

⚠ Due to the large number of options, no contextual information is provided.

Phishing - T1566 | Custom Cryptographic Protocol - T1024 | Command and Scripting Interpreter - T1059 | Indirect Command Execution - T1202 | Masquerading - T1036 | Deobfuscate/Decode Files or Information - T1140 | Windows Command Shell - T1059.003 |

Submit

Once you have added all the techniques and clicked Submit

Galaxies

Attack Pattern

Masquerading - T1036 | Phishing - T1566 | Custom Cryptographic Protocol - T1024 | Command and Scripting Interpreter - T1059 | Windows Command Shell - T1059.003 | Deobfuscate/Decode Files or Information - T1140 | Indirect Command Execution - T1202 |

Galaxies User

« previous next » view all

+ Scope Deleted Decay Cluster attached Context

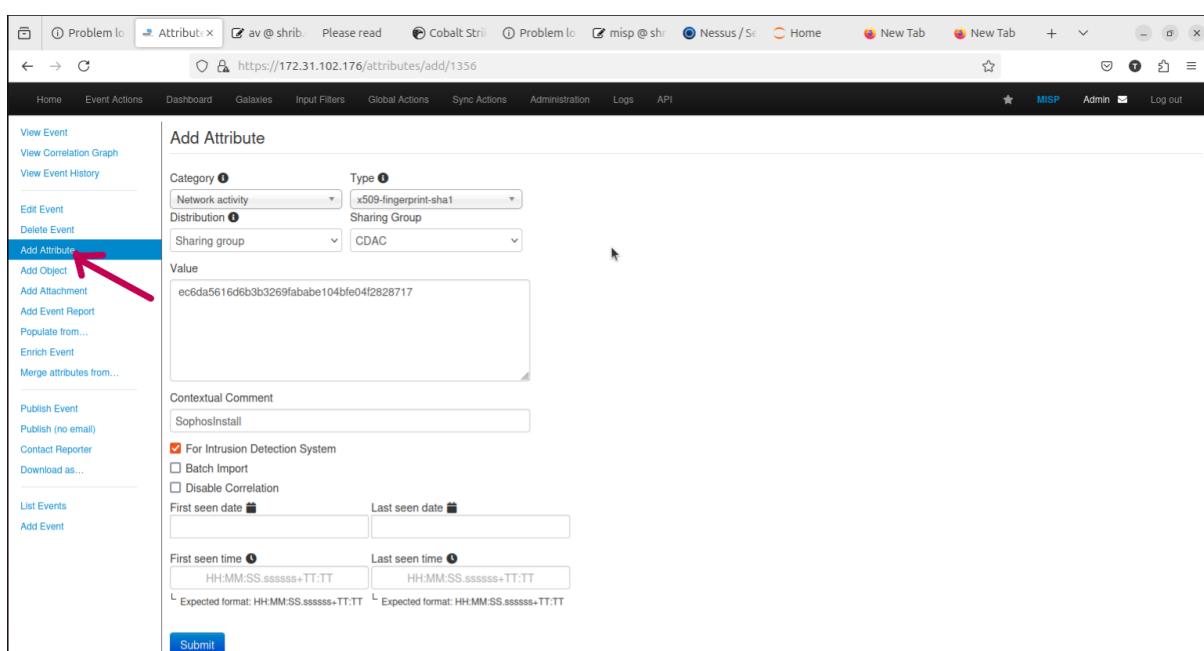
you will see them populated in the Event view.

6 Populating an Event

MISP attributes are atomic pieces of intelligence, such as network indicators (e.g., IP addresses, domains, URLs), system indicators (a string in memory, a file hash, etc.), or even a Bitcoin wallet. An attribute will have a type that describes it and an overarching category that puts it in context (making it intelligence rather than just data). You can add the Intrusion Detection System (IDS) flag to an attribute to determine if an attribute can be automated (such as being exported as an IDS ruleset or used for detection).

6.1 Adding MISP Attributes

- To add an attribute to an Event, select the Add Attribute button from the left-hand menu.
- You can then fill out the Add Attribute web form to provide context to the attribute you add. First, choose what Category the attribute falls under, then choose the Type of attribute and how you want to share this attribute (Distribution). You can then copy and paste the Value across.



The screenshot shows the 'Add Attribute' form in the MISP interface. The sidebar on the left has a red arrow pointing to the 'Add Attribute' button. The main form includes fields for Category (Network activity), Type (x509-fingerprint-sha1), Distribution (Sharing Group), Value (ec6da5616d6b3b3269fababe104bfe04f2828717), Contextual Comment (SophosInstall), and checkboxes for 'For Intrusion Detection System', 'Batch Import', and 'Disable Correlation'. It also includes date and time input fields for 'First seen date' and 'Last seen date', and dropdowns for 'First seen time' and 'Last seen time' with expected formats HH:MM:SS.ssssss+TT:TT. A 'Submit' button is at the bottom.

When you are done filling out the attribute details, click the Submit button. This will add the attribute(s) you created to the MISP Event. Scrolling down the View Event page, you can see these attributes listed. You can add attributes directly from this view by clicking the Add attribute button (+ icon) here.



Value	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed hits	IDS	Distribution	Sightings	Activity
2025-01-30		Network activity	x509-fingerprint-sha1	ec6da5616d6b3b3269fababe104bfe04f2828717				<input checked="" type="checkbox"/>	1355	<input checked="" type="checkbox"/>	CDAC			(0 0)

6.2 Automated Data Upload

- Although you can create objects and attributes manually, MISP offers easier ways to add intelligence to an Event.
- Select Populate from in the left-side menu brings up a popup window where you can choose to populate the MISP Event using automated methods

The screenshot shows the MISP web interface with a sidebar on the left containing various event management links. One link, 'Populate from...', is highlighted with a red arrow. The main content area displays an event titled 'Covert Delivery of Cobalt Strike Beacon via Sophos Phishing Website'. The event details include fields like Event ID (1356), UUID (295eadd2-2827-4f67-8172-be2a41b1502), Creator org (ORGNAME), and Tags (OSINT, tip:white). A red box highlights a warning message: 'The event is tagged as tip:white, yet the distribution is not set to all. Change the distribution setting to something more lax if you wish for the event to propagate further.' On the right, there's a 'Related Events' section showing a single entry for 'covert cobalt' from 2025-01-29.

The two most common import methods you are likely to use are Populate using a Template which lets you use a custom template to make it easier to upload attributes to MISP, and the Freetext Import. Let's take a look at the Freetext Import tool.

The screenshot shows a modal dialog box titled 'Choose the format that you would like to use for the import'. It lists several options: 'Populate using a JSON file containing MISP event content data' (disabled), 'Freetext Import' (selected and highlighted with a red box), 'Populate using a Template' (disabled), 'OpenIOC Import' (disabled), 'ThreatConnect Import' (disabled), '(Experimental) Forensic analysis - Mactime' (disabled), and 'Cancel'. The background of the main interface shows the same event details as the previous screenshot.

Copy and paste the IOCs into the Freetext Import tool from your source and click Submit:

The screenshot shows the Freetext Import Tool interface. A text area contains the following IOCs:

```
c974ffe23][57ec909ef26b55f202047e ec6da5616d6b3b3269fababe104bfe04f2828717
067c95ad074afdb8993281b02f74d0f257fb312943da0887355da652afb54c0ab MD5
SHA1
SHA256 SophosInstall..exe
sopbos[.]com Domain Phishing Site
98[.]71.232[.]223 IP C&C
```

Below the text area are two buttons: "Submit" and "Cancel". At the bottom of the window, there are several tabs: INT, tip:white, and a few others.

The Freetext Import tool will parse these IOCs into legitimate MISP attributes. However, it might not get it right every time. As such, the tool lets you change your attributes before adding them to your Event in a review screen.

The screenshot shows the Freetext Import Results page. It displays a table of parsed attributes:

Value	Similar Attributes	Category	Type	IDS	Disable Correlation	Distribution	Comments
c974ffe23][57ec909ef26b55f202047e	1355	Payload delivery	md5	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit event	
ec6da5616d6b3b3269fababe104bfe04f2828717	1355 1356	Payload delivery	sha1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit event	
067c95ad074afdb8993281b02f74d0f257fb312943da0887355da652afb54c0ab	1355	Payload delivery	sha256	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit event	
SophosInstall..exe	1355	Payload delivery	filename	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit event	
sopbos.com	1355	Network activity	domain	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit event	
98.71.232.223	1355	Network activity	ip-dst	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Inherit event	

Below the table are buttons for "Submit attributes", "Change all", and "Update all comment fields".

Clicking the Submit attributes button will add the attributes to the MISP event, which you can then view on the Event View page.

The screenshot shows the Event View page with the following table of attributes:

Date	Org	Category	Type	Value	Tags	Galaxies	Comment	Correlate	Related	Feed	IDS	Distribution	Sighting Events	hits
2025-01-30		Payload delivery	md5	c974ffe23][57ec909ef26b55f202047e	[+]	[+]	[+]	<input checked="" type="checkbox"/>	1355	<input checked="" type="checkbox"/>	Inherit		(0 0 0)	
2025-01-30		Payload delivery	sha1	ec6da5616d6b3b3269fababe104bfe04f2828717	[+]	[+]	[+]	<input checked="" type="checkbox"/>	1355	<input checked="" type="checkbox"/>	Inherit		(0 0 0)	
2025-01-30		Payload delivery	sha256	067c95ad074afdb8993281b02f74d0f257fb312943da0887355da652afb54c0ab	[+]	[+]	[+]	<input checked="" type="checkbox"/>	1355	<input checked="" type="checkbox"/>	Inherit		(0 0 0)	
2025-01-30		Payload delivery	filename	SophosInstall..exe	[+]	[+]	[+]	<input checked="" type="checkbox"/>	1355	<input checked="" type="checkbox"/>	Inherit		(0 0 0)	
2025-01-30		Network activity	domain	sopbos.com	[+]	[+]	[+]	<input checked="" type="checkbox"/>	1355	<input checked="" type="checkbox"/>	Inherit		(0 0 0)	
2025-01-30		Network activity	ip-dst	98.71.232.223	[+]	[+]	[+]	<input checked="" type="checkbox"/>	1355	<input checked="" type="checkbox"/>	Inherit		(0 0 0)	

MISP's Freetext Import option is a powerful tool that makes it very easy to upload a large number of IOCs in one go, rather than having to manually upload individual attributes or objects. The tool also lets you customize how attributes are uploaded. For instance, you could have created a file object out of those file hashes to link them to the same filename using the Create object button. I highly recommend using this tool, or creating a custom template, when uploading data to MISP.

7 Creating Multiple Users and allowing them to communicate on a shared malware

1. Log in to your MISP instance as an administrator.
2. Navigate to **Administration → List Users**.
3. Click on **Add User** in the top-right corner.
4. Fill in the user details:
 - **Email:** Enter the user's email address.(user@user.test)
 - **Organisation:** Select the appropriate organization.(shared group - CDAC)
 - **Role:** Choose the role (User), as admin is already registered
 - **Password:** Set a strong password.
5. Click **Submit** to create the user.
6. Repeat the above steps for each additional user.

The screenshot shows the MISP administration interface. The left sidebar has a 'List Users' section highlighted. The main area displays a table of users with columns: Tags, Galaxies, Comment, Correlate, Related, Feed, IDS, Distribution, Sighting Events, and hits. A new user entry is visible in the table, showing 'Inherit' under 'IDS' and 'CDAC' under 'Distribution'. A red arrow points from the 'Add User' button in the sidebar to this new entry in the table.

after adding users you can now see them on clicking list user

The screenshot shows the MISP administration interface with the 'List Users' section in the sidebar highlighted. The main area is titled 'Users index' and shows a table of users. The table includes columns for Event alert, Contact alert, PGP Key, NIDS SID, Terms Accepted, Last Login, Created, and Disabled. A red arrow points from the 'List Users' button in the sidebar to the 'Event alert' column in the table.

8 Decaying Model Tools

Decaying models help prioritize threat intelligence over time by reducing the relevance of older data. Several tools can be used for implementing decay models in MISP.

8.1 Step 1: Understanding Decaying Models

Decaying models assign a confidence score to attributes based on their age and impact. This helps analysts focus on the most relevant data.

8.2 Step 2: Available Decaying Tools

- **MISP Decaying Model:** Built-in MISP feature that allows attribute decay configuration based on event types.
- **Custom Decay Scripts:** Python scripts can be used to create custom decay logic tailored to organizational needs.
- **Machine Learning Models:** Advanced models can be trained to predict decay patterns based on historical data.

8.3 Step 3: Configuring Decay in MISP

To configure decay models in MISP:

1. Navigate to **Global Actions** → decaying models list.

The screenshot shows the MISP web interface. At the top, there is a navigation bar with links for Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions (highlighted with a red box), Sync Actions, Administration, Logs, and API. On the right side of the header, there are user icons for MISPL, Admin, and Logout. Below the header, the main content area displays an event details page for "Covert Delivery of Cobalt Strike via Sophos Phishing Website". The event ID is 1356, and it was created on 2025-01-29 by ORGANIZATION. The distribution is set to CDAC. A warning message states: "The event is not published yet. Please publish it if you want to share it with others." A red box highlights the "Decaying Models Tool" link under the "Decaying Models" section of the sidebar. Another red box highlights the "Decaying Models" link in the same sidebar. To the right of the event details, there is a "Related Events" sidebar showing a list of other events, with one entry for "covert cobalt" from 2025-01-29 and another for "Malspam 2017-06-21 Job Application" from 2017-06-21.

2. Locate the **Decaying Model** settings.

3. Click the Update Default Models options from the left-side menu to load the default decaying models that come with MISP.

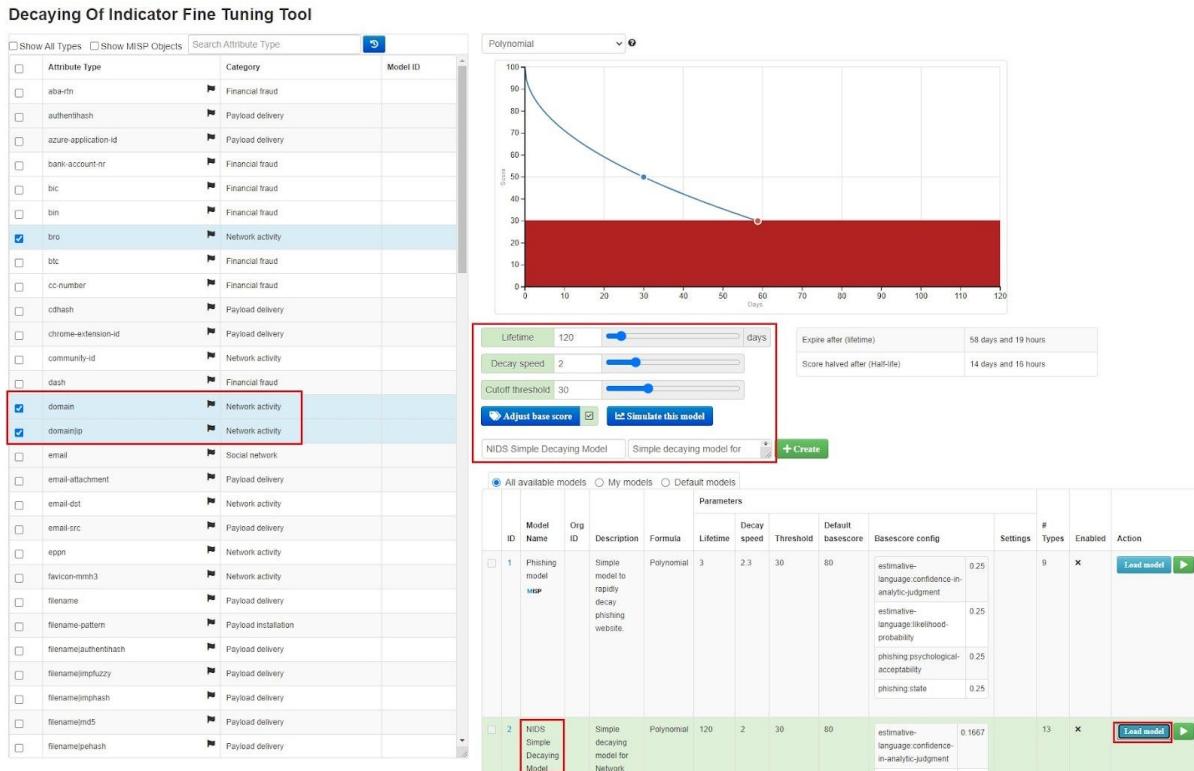
ID	Organization	Usable to	Name	Description	Parameters []	Formula	# Assigned Types	Version	Enabled	Actions
1	MISP	✓	Phishing model	Simple model to rapidly decay phishing website.	{"lifetime":3,"decay_speed":2.3,"threshold":30,"default_base_score":80,"base_score_config":{"estimative-language:confidence-in-analytic-judgment":0.25,"estimative-language:likelihood-probability":0.25,"phishing:psychological-acceptability":0.25,"phishing:state":0.25}}	Polynomial	9	2	x	
2	MISP	✓	NIDS Simple Decaying Model	Simple decaying model for Network Intrusion Detection System (NIDS).	{"lifetime":120,"decay_speed":2,"threshold":30,"default_base_score":80,"base_score_config":{"estimative-language:confidence-in-analytic-judgment":0.1667,"estimative-language:likelihood-probability":0.1667,"false-positive-risk":0.1667,"priority-level":0.1667,"retention":0.1667,"targeted-threat-index:targeting-sophistication-base-value":0.0833,"targeted-threat-index:technical-sophistication-multiplier":0.0833}}	Polynomial	13	2	x	
3	MISP	✓	Vishing model	Simple model to rapidly decay voice scamming, vishing relying on phone-numbers.	{"lifetime":10,"decay_speed":2.3,"threshold":30,"default_base_score":80,"base_score_config":{"estimative-language:confidence-in-analytic-judgment":0.25,"estimative-language:likelihood-probability":0.25,"phishing:psychological-acceptability":0.25,"phishing:state":0.25}}	Polynomial	2	1	x	

4. This will populate the Decaying Models screen with a list of the default models that come with every MISP install. You can use the buttons under the Actions column to view, download, edit, and enable the models.

5. You can add your own decaying model or import one using the options on the left-side menu. However, for now, we will just apply a default one to our MISP attributes. To do this, first select the Decaying Models Tool option in the left-side menu.

ID	Organization	Usable to	Name	Description	Parameters []	Formula	# Assigned Types	Version	Enabled	Actions
1	MISP	✓	Phishing model	Simple model to rapidly decay	{"lifetime":3,"decay_speed":2.3,"threshold":30,"default_base_score":80,"base_score_config":{"estimative-language:confidence-in-analytic-judgment":0.25,"estimative-language:likelihood-probability":0.25}}	Polynomial	9	2	v	

6. You can choose to select multiple attributes, assign these factors to them, and then create your own decaying model using the Create button. However, using one of the default decaying models MISP provides is the easiest way. To do this, scroll down to the model you want to use and select Load model. This will load the model into the fine tuning tool, where you can see which attributes it affects and how it affects them. Here, I have selected the NIDS Simple Decaying Model, which affects network indicators.



7. Once enabled, you will now see a Score field next to the MISP attributes that relate to the decaying model you enabled. This reflects the current value an attribute has, and it will decrease over time. Navigate to an Event and click the Decay score button to see this.

ID	Event Title	Attributes
ec6da5616d6b3b3269fababe104bfe04f2828717	ab	(0:0:0)
c974ffe23d57ec909ef26b55f202047e		(0:0:0)
SophosInstall.exe		(0:0:0)
sopbos.com		Phishing model 33.07 NIDS Simple Decaying ... 73.15
98.71.232.223		Phishing model 33.07 NIDS Simple Decaying ... 73.15
ec6da5616d6b3b3269fababe104bfe04f2828717	SophosInstall	(0:0:0)

this concludes the basics of misp

9 Steps to Generate API Key for Automation and Integration

1. Log in to your MISP instance as an administrator.
2. Navigate to **Administration → List Auth keys**.
3. Find the user for whom you want to generate an API key.
4. Click on the **Edit** button next to the user's name.
5. Scroll down to the API key section.
6. Click on **Generate new authentication key**.
7. Copy and securely store the generated API key.

The screenshot shows the MISP Administration interface. On the left, there is a sidebar with various management links. The main area is titled 'Authentication key Index' and displays a table of existing API keys. One row is highlighted, and a red arrow points from step 6 to the '+ Add authentication key' button. Another red arrow points from step 4 to the 'Edit' button next to the user 'admin@admin.test'. The right side of the screen shows a sidebar with more administration options like 'List Users' and 'Logs'.

#	User	Auth Key
1	admin@admin.test	JO8v*****IXUA
3	admin@admin.test	9c40*****e78y

10 Automation for Advanced Threat Detection and Intelligence Module

10.1 Fetch Threat Feeds from OSINT Sources

Purpose: Retrieve actionable intelligence such as malicious IPs, domains, and hashes from public and private threat intelligence platforms.

1. MISP API: Retrieve and process threat intelligence events.
2. AlienVault OTX API: Fetch reputation details for IPs/domains.
3. VirusTotal API: Check file hashes, URLs, or IPs for known threats.

11 Steps to Integrate AlienVault OTX with MISP

11.1 Prerequisites

- A running instance of MISP.
- An active AlienVault OTX account.
- API key from AlienVault OTX.

11.2 Configuring MISP to Fetch Data from OTX

1. Log in to your MISP instance as an administrator.
2. Navigate to **Sync Actions → List Feeds**.
3. Click on **Add Feed** and configure the following:
 - **Name:** AlienVault OTX
 - **URL:** Provide the appropriate OTX feed URL.
 - **Enabled:** Yes
 - **Source Format:** MISP Feed

4. Click **Submit** to save the configuration.

Add Feed
Import feeds from JSON
Feed overlap analysis matrix
Export Feed settings

View Feed

Add a new MISP feed source.
 Enabled
 Caching enabled
 Lookup visible

Name: AlienVaultOTX

Provider: Alien Vault

Input Source: Network

URL: https://otx.alienvault.com/api/v1/pulses/subscribed

Source Format: MISP Feed

Any headers to be passed with requests (example: Authorization):
Authorization: [REDACTED]

Add Basic Auth

Distribution: Sharing group

Sharing Group

5. Navigate to **Sync Actions** → **Fetch Feeds** and click **Fetch and Store** to pull data from OTX.

List Feeds
Search feed caches
Add Feed
Import Feeds from JSON
Feed overlap analysis matrix
Export Feed settings

Feeds

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

Load default feed metadata Cache all feeds Cache freeText/CSV feeds Cache MISP feeds Fetch and store all feed data

ID	Enabled	Caching	Name	Format	Provider	Org	Source	URL	Headers
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	CIRCL OSINT	misp	CIRCL	network		https://www.circl.lu/doc/misp/feed-osint	
18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	alienvault	csv	.alienvault.com	network		https://reputation.alienvault.com/reputation.generic	
74	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	AlienVaultOTX	misp	Alien Vault	network		https://otx.alienvault.com/	Authorization: [REDACTED]

6. Verify that the fetched data is available in the **Events** section.

<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME	1313	Attack Pattern	<input checked="" type="checkbox"/> Exploit Public-Facing Application - T1190	<input checked="" type="checkbox"/> PAP:CLEAR	<input checked="" type="checkbox"/> tip:white	<input checked="" type="checkbox"/> type:OSINT	<input checked="" type="checkbox"/> osint:lifetime="perpetual"	<input checked="" type="checkbox"/> tip:clear
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME	1312	Country	<input checked="" type="checkbox"/> china	<input checked="" type="checkbox"/> type:OSINT	<input checked="" type="checkbox"/> osint:lifetime="perpetual"	<input checked="" type="checkbox"/> osint:certainity="50%"	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME	1311	Attack Pattern	<input checked="" type="checkbox"/> Exploit Public-Facing Application - T1190	<input checked="" type="checkbox"/> type:OSINT	<input checked="" type="checkbox"/> osint:lifetime="perpetual"	<input checked="" type="checkbox"/> osint:certainity="50%"	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME	1310	Attack Pattern	<input checked="" type="checkbox"/> Phishing - T1566	<input checked="" type="checkbox"/> type:OSINT	<input checked="" type="checkbox"/> osint:lifetime="perpetual"	<input checked="" type="checkbox"/> osint:certainity="50%"	<input checked="" type="checkbox"/> phishing:techniques="fake-website"	<input checked="" type="checkbox"/> phishing:state="unknown"
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME	1309	Attack Pattern	<input checked="" type="checkbox"/> Exploit Public-Facing Application - T1190	<input checked="" type="checkbox"/> type:OSINT	<input checked="" type="checkbox"/> osint:lifetime="perpetual"	<input checked="" type="checkbox"/> tip:white	<input checked="" type="checkbox"/> tip:clear	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME	1308		<input checked="" type="checkbox"/> type:OSINT	<input checked="" type="checkbox"/> osint:lifetime="perpetual"	<input checked="" type="checkbox"/> tip:white	<input checked="" type="checkbox"/> tip:clear		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	ORGNAME	1304	Country	<input checked="" type="checkbox"/> china	<input checked="" type="checkbox"/> type:OSINT	<input checked="" type="checkbox"/> osint:lifetime="perpetual"	<input checked="" type="checkbox"/> tip:white	<input checked="" type="checkbox"/> tip:clear	
<input type="checkbox"/>	<input checked="" type="checkbox"/>			Attack Pattern	<input checked="" type="checkbox"/> Compromise Software Supply Chain - T1195.002	<input checked="" type="checkbox"/> type:OSINT	<input checked="" type="checkbox"/> osint:lifetime="perpetual"	<input checked="" type="checkbox"/> tip:white	<input checked="" type="checkbox"/> tip:clear	

Page 1 of 23, showing 60 records out of 1356 total, starting on record 1, ending on 60

< previous 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 next >

Now, to add virusTotal integration in misp , we need to install misp modules in our misp vm

Once the virtual environment is loaded, use the following command to install MISP modules:

12 Installing MISP Modules

MISP modules extend the functionality of MISP by providing additional enrichment and expansion features. The following steps outline the installation and configuration of MISP modules.

12.1 Step 1: Install MISP Modules

Once the virtual environment is loaded, use the following command to install MISP modules:

```
pip install misp-modules
```

12.2 Step 2: Install System Dependencies

On Ubuntu, install the required system dependencies:

```
sudo apt install libpoppler-cpp-dev libzbar0 tesseract-ocr
```

For an updated list of dependencies, check the GitHub workflow inside .github/workflows.

12.3 Step 3: Install Additional Python Packages

Some dependencies are not installed by default due to PyPI limitations. Install them manually using:

```
pip install \
git+https://github.com/cartertemm/ODTReader.git \
git+https://github.com/abenassi/Google-Search-API \
git+https://github.com/SteveClement/trustar-python.git \
git+https://github.com/sebdraven/pydnstrails.git \
git+https://github.com/sebdraven/pyonyphe.git
```

12.4 Step 4: Run MISP Modules

After installation, you can start MISP modules with the following command:

misp—modules

If necessary, reload the virtual environment to update the search path for executables.

12.5 Step 4: Run MISP Modules

After installation, you can start MISP modules with the following command:

misp—modules

If necessary, reload the virtual environment to update the search path for executables.

13 Enriching Events with VirusTotal

Once MISP modules are installed, you can use the VirusTotal enrichment module to gather additional threat intelligence. Follow these steps to configure and use it:

13.1 Step 1: Enable the VirusTotal Module

eginenumerate

Log in to your MISP instance as an administrator.

Navigate to Administration → Server Settings → Plugin Settings.

The screenshot shows the MISP administration interface. The left sidebar has links for Add User, List Users, Pending registrations, User settings, Set Setting, Contact Users, Add Organisation, List Organisations, Add Role, List Roles, Server Settings & Maintenance (which is selected), and Update Progress. The top navigation bar includes Home, Event Actions, Dashboard, Galaxies, Input Filters, Global Actions, Sync Actions, Administration, Logs, API, and Admin. The main content area is titled 'Server Settings & Maintenance' and contains tabs for Overview, MISP settings (9), Encryption settings (4), Proxy settings (5), Security settings (5), **Plugin settings (541)**, SimpleBackgroundJobs settings, Diagnostics, Manage files, and Workers (1). Below the tabs, there are sections for Enrichment, Import, Export, Cortex, Sightings, CyCat, and RPZ. Red arrows highlight the 'Server Settings & Maintenance' link in the sidebar, the 'Plugin settings' tab in the top navigation, and the 'RPZ' link in the sidebar.

Find the section related to Enrichment and ensure that the VirusTotal module is enabled with the following configurations.

Save the settings.

13.2 Step 2: Configure API Key

VirusTotal requires an API key for querying its database. Obtain an API key from VirusTotal and configure it in MISP:

1. Go to <https://www.virustotal.com/gui/home/upload> and sign in.
2. Retrieve your API key from your account settings.
3. In MISP, navigate to **Administration → Plugin Settings**.
4. Locate the VirusTotal module settings and enter your API key.

Recommended	Plugin.Enrichment_virustotal_public_enabled	true	Enable or disable the virustotal_public module.
Recommended	Plugin.Enrichment_virustotal_public_restrict	ORGNAME	Restrict the virustotal_public module to the given organisation.
Recommended	Plugin.Enrichment_virustotal_public_apikey	[REDACTED]	Set this required module specific setting.
Recommended	Plugin.Enrichment_virustotal_public_proxy_host		Set this required module specific setting.
Recommended	Plugin.Enrichment_virustotal_public_proxy_port		Value not set.

5. Save the configuration.

13.3 Step 3: Enrich an Event Using VirusTotal

eginenumerate

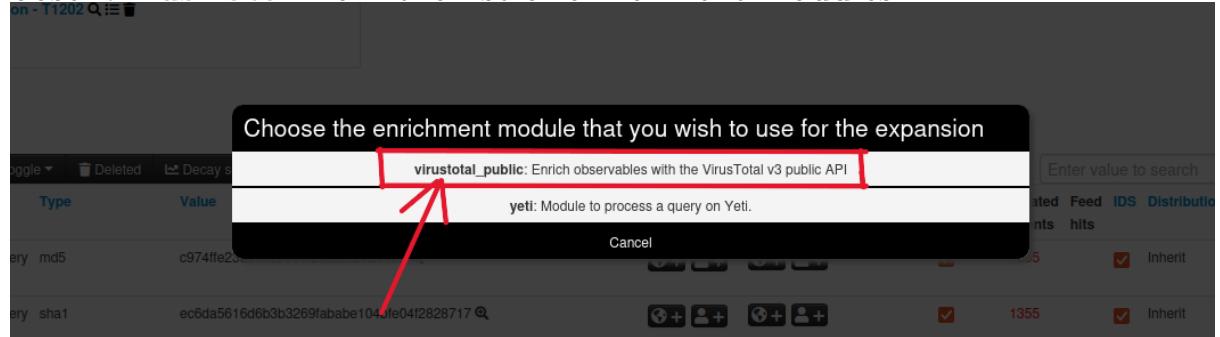
Navigate to an existing MISP event or create a new one.

Add an attribute such as a file hash, domain, or IP address.

Click on the attribute and select **Enrich**.

Date	Org	Type	Value	Tags	Galaxies	Comment	Correlate	Related Events	Feed	IDS	Distribution	Sightings	Propose enrichment
2025-01-30		Payload delivery	md5:c974ffe23d57ec909ef2eb055f202047e	[Tags]	[Galaxies]		<input checked="" type="checkbox"/>	1355	<input checked="" type="checkbox"/>	Inherit	(0 0)		
2025-01-30		Payload delivery	sha1:ec6da5616d6b3b3269fababe104bfe0412828717	[Tags]	[Galaxies]		<input checked="" type="checkbox"/>	1355	<input checked="" type="checkbox"/>	Inherit	(0 0)		
2025-01-30		Payload delivery	sha256:067c95ad074afdb993281b02f74d0f257fb312943da0887355da652ab54c0ab	[Tags]	[Galaxies]		<input checked="" type="checkbox"/>	1355	<input checked="" type="checkbox"/>	Inherit	(0 0)		
2025-01-30		Payload delivery	filename:SophosInstall.exe	[Tags]	[Galaxies]		<input checked="" type="checkbox"/>	1355	<input checked="" type="checkbox"/>	Inherit	(0 0)		
2025-01-30		Network activity	domain:sopbos.com	[Tags]	[Galaxies]		<input checked="" type="checkbox"/>	1355	<input checked="" type="checkbox"/>	Inherit	(0 0)		
2025-01-30		Network activity	ip-dst:98.71.232.223	[Tags]	[Galaxies]		<input checked="" type="checkbox"/>	1355	<input checked="" type="checkbox"/>	Inherit	(0 0)		
2025-01-30		x509-fingerprint-sha1	ec6da5616d6b3b3269fababe104bfe0412828717	[Tags] SophosInstall	[Galaxies]		<input checked="" type="checkbox"/>	1355	<input checked="" type="checkbox"/>	CDAC	(0 0)		

Choose **VirusTotal** from the list of enrichment modules.



Wait for the enrichment process to complete and review the additional data fetched from VirusTotal.

13.4 Step 4: Review and Utilize the Enriched Data

1. After enrichment, MISP will display additional threat intelligence from VirusTotal.

The screenshot shows the "Enrichment Results" page. On the left, there is a sidebar with various options like View Event, Edit Event, Add Attribute, etc. The main area is titled "Enrichment Results" and contains a table of enriched objects. The table has columns for Import, Category, Type, Value, Tags, IDS, Disable, Comment, and Distribution. Some rows are expanded to show more details, such as external analysis results and network activity logs. Each row has checkboxes for Tags, IDS, and Disable, and dropdown menus for Comment and Distribution.

Import	Category	Type	Value	Tags	IDS	Disable	Comment	Distribution
External analysis	detection-ratio	Name:	virustotal-report	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	c974ffe23d57ec909ef26b55f202c	Inherit event
		References:	0				c974ffe23d57ec909ef26b55f202c	Inherit event
		External analysis	permalink link				https://www.virustotal.com/gui/file/067c95ad074a0d8993281b02f74d0f257fb312943da0887355da652aef54c0ab	c974ffe23d57ec909ef26b55f202c
External analysis	detection-ratio	External analysis	detection-ratio text	50/75	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	c974ffe23d57ec909ef26b55f202c	Inherit event
		Name:	virustotal-report	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	c974ffe23d57ec909ef26b55f202c	Inherit event	
		References:	0	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	c974ffe23d57ec909ef26b55f202c	Inherit event	
Network activity	domain	domain	tp2e7a.wpc.2be4.phicdn.net	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	c974ffe23d57ec909ef26b55f202c	Inherit event
							Name:	domain-ip
Network activity	domain	domain	tp2e7a.wpc.2be4.phicdn.net	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	c974ffe23d57ec909ef26b55f202c	Inherit event
							Name:	domain-ip

2. Review the information to assess threats and take appropriate action, scroll down and click submit.

<input checked="" type="checkbox"/> External analysis detection-ratio text 0/94		<input type="checkbox"/> c974ffe23d57ec909ef26b55f2020 [Inherit event]
<input checked="" type="checkbox"/> Name: domain-ip <small>□</small> References: 0		<input type="checkbox"/> c974ffe23d57ec909ef26b55f2020 [Inherit event]
<input checked="" type="checkbox"/> Network activity IP ip-dst 204.79.197.200	<input checked="" type="checkbox"/> <input type="checkbox"/> c974ffe23d57ec909ef26b55f2020 [Inherit event]	
<input checked="" type="checkbox"/> Name: virustotal-report <small>□</small> References: 0		<input type="checkbox"/> c974ffe23d57ec909ef26b55f2020 [Inherit event]
<input checked="" type="checkbox"/> External analysis permalink link https://www.virustotal.com/gui/ip_address/23.216.147.64	<input checked="" type="checkbox"/> <input type="checkbox"/> c974ffe23d57ec909ef26b55f2020 [Inherit event]	
<input checked="" type="checkbox"/> External analysis detection-ratio text 1/94	<input checked="" type="checkbox"/> <input type="checkbox"/> c974ffe23d57ec909ef26b55f2020 [Inherit event]	
<input checked="" type="checkbox"/> Name: domain-ip <small>□</small> References: 0		<input type="checkbox"/> c974ffe23d57ec909ef26b55f2020 [Inherit event]
<input checked="" type="checkbox"/> Network activity IP ip-dst 23.216.147.64	<input checked="" type="checkbox"/> <input type="checkbox"/> c974ffe23d57ec909ef26b55f2020 [Inherit event]	
<input checked="" type="checkbox"/> Name: file <small>□</small> References: 0		<input type="checkbox"/> c974ffe23d57ec909ef26b55f2020 [Inherit event]
<input checked="" type="checkbox"/> Payload delivery md5 md5 c974ffe23d57ec909ef26b55f202047e	<input checked="" type="checkbox"/> <input type="checkbox"/> c974ffe23d57ec909ef26b55f2020 [Inherit event]	
<input checked="" type="checkbox"/> Payload delivery sha1 sha1 ec6da561646b3b03269fababe104bf0412828717	<input checked="" type="checkbox"/> <input type="checkbox"/> c974ffe23d57ec909ef26b55f2020 [Inherit event]	
<input checked="" type="checkbox"/> Payload delivery sha256 sha256 067c95ad074ad08993281b02f74d0f257fb312943da0887355da652ab54c0ab	<input checked="" type="checkbox"/> <input type="checkbox"/> c974ffe23d57ec909ef26b55f2020 [Inherit event]	
<input checked="" type="checkbox"/> Payload delivery tish tish T19FB3A946F89400EE23F9BB96DF5142646726E52F189DB4A088DBF7E4 D33704DE4222F	<input checked="" type="checkbox"/> <input type="checkbox"/> c974ffe23d57ec909ef26b55f2020 [Inherit event]	
<input checked="" type="checkbox"/> Payload delivery vhash vhash 015026557z	<input checked="" type="checkbox"/> <input type="checkbox"/> c974ffe23d57ec909ef26b55f2020 [Inherit event]	
<input checked="" type="checkbox"/> Payload delivery ssdeep ssdeep 15362EHQmM3NJK3l/5CxGk0Ua6oAm3gWl59xxYalgrnjbYnbwjrsw+A0U0 RlD:qqvM3Xl/5CxGkFMT9xojmsgdnjlsD	<input checked="" type="checkbox"/> <input type="checkbox"/> c974ffe23d57ec909ef26b55f2020 [Inherit event]	

Submit Cancel

- Now, you can check the enriched data in attributes section of Events in Misp.

<small>Windows Command Shell - T1059.003</small> <small>Deobfuscate/Decode Files or Information - T1140</small> <small>Indirect Command Execution - T1202</small>	
Date	Object name: file
	References: 0
2025-01-31	
<input type="checkbox"/>	Object name: file <small>□</small> References: 0
<input type="checkbox"/> 2025-01-31	Payload delivery md5: md5 c974ffe23d57ec909ef26b55f202047e
<input type="checkbox"/> 2025-01-31	Payload delivery sha1: sha1 ec6da561646b3b03269fababe104bf0412828717
<input type="checkbox"/> 2025-01-31	Payload delivery sha256: sha256 067c95ad074ad08993281b02f74d0f257fb312943da0887355da652ab54c0ab
<input type="checkbox"/> 2025-01-31	Payload delivery tish: tish T19FB3A946F89400EE23F9BB96DF5142646726E52F189DB4A088DBF7E4 D33704DE4222F
<input type="checkbox"/> 2025-01-31	Payload delivery vhash: vhash 015026557z

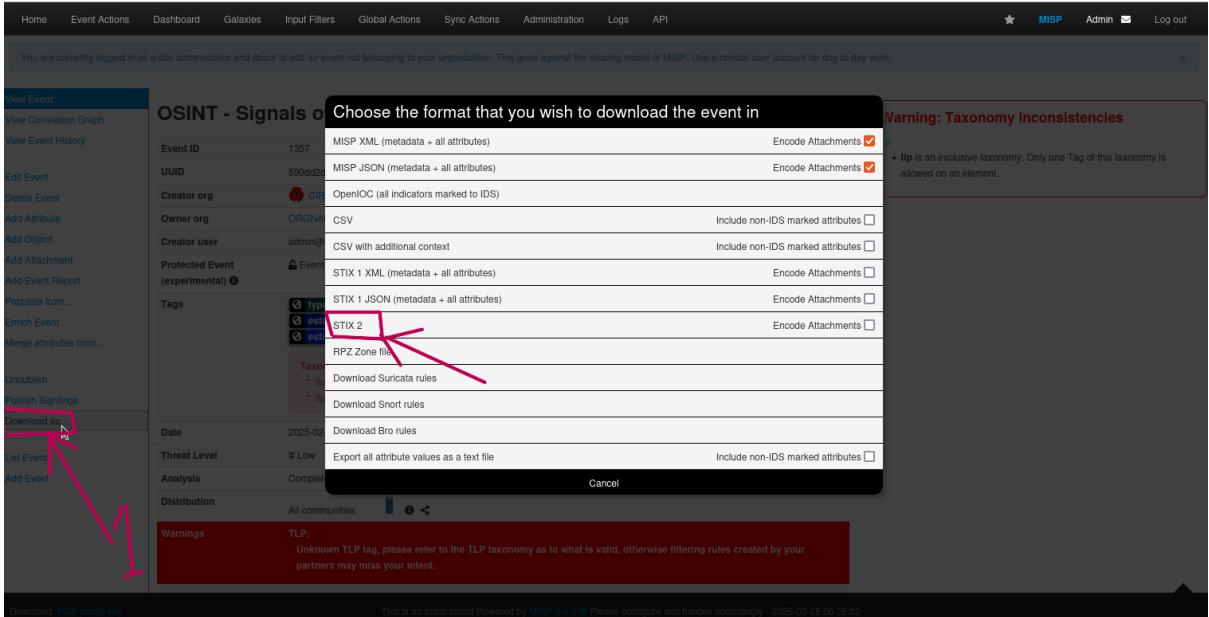
you can scroll down to check all the enriched data.

- If needed, correlate the new data with other MISP events for deeper analysis.

14 Correlate Threat Feeds with Vulnerabilities

14.1 Prerequisites for performing Correlation

1. Misp Events should be available in stix-2 format for downloading



if you are unable to download then use the following commands in your misp VM to be to download the required MISP event stix-2 format

```
sudo apt update
pip install stix2
sudo apt install jq curl
```

2. once you are able to download the misp event in stix2 format now need to get data from NVD or you can also perform a nessus scan in your system

```
curl -s "https://services.nvd.nist.gov/rest/json/cves/2.0?pubStartDate=2024-01-01T00:00:00.000&pubEndDate=2024-01-30T23:59:59.999&resultsPerPage=500" | jq -c '.vulnerabilities[] | { index: { _index: "nvd-cves" } }, .' > nvd_cves.json
```

This fetches CVEs published between 01-01-2024 and 30-01-2024 and formats them for Elasticsearch bulk upload.

3. you can also perform nessus system scan to fetch all the necessary IOCS for correlation
4. once you get the file of CVEs/IOCS from nessus or NVD (using above command) then you need to format the NVD-CVE file using this script.

```

python3 - <<EOF
import json

# Load the original JSON file
input_file = "/home/musharaf-misp-admin/
    musharaf/misp scan_f20myj.nessus"
output_file = "/home/musharaf-misp-admin/
    nessus_cve_bulk.json"

with open(input_file, "r", encoding="utf-8") as
    file:
    data = json.load(file)

# Extract CVE data
cve_list = data.get("vulnerabilities", [])

# Convert to Elasticsearch bulk format
bulk_data = ""
for item in cve_list:
    cve = item.get("cve", {})
    cve_id = cve.get("id", "UNKNOWN")
    bulk_data += json.dumps({"index": {"_index"
        : "nvd_cve_index", "_id": cve_id}}) + "\n"
    bulk_data += json.dumps(cve) + "\n"

# Save to bulk file
with open(output_file, "w", encoding="utf-8") as
    bulk_file:
    bulk_file.write(bulk_data)

print(f"Bulk data saved to {output_file}")
EOF

```

```
Bulk data saved to /home/musharaf-misp-admin/
nvd_cve_bulk.json
```

5. since you have two files now misp-event in stix2 format and NVD-cves file in desired format for correlation, next we will continue with ELK installation that is **elasticsearch logstash kibana** which is a SIEM tool.

15 ELK Stack for Threat Intelligence Correlation

The ELK Stack (Elasticsearch, Logstash, and Kibana) is widely used for real-time data analysis and visualization. In the context of threat intelligence, ELK enables efficient correlation of **Indicators of Compromise (IOCs) with vulnerabilities (CVEs)**.

- **Elasticsearch** serves as a distributed search engine to store and query threat intelligence data efficiently.
- **Logstash** helps process and ingest structured/unstructured security logs.
- **Kibana** provides an interactive UI to visualize the correlated data.

By using ELK, we can:

- Store threat intelligence data from MISP, VirusTotal, and Nessus in Elasticsearch.
- Correlate extracted CVEs with threat indicators (IPs, domains, hashes).
- Visualize trends, attack patterns, and vulnerability exposures using Kibana.

15.1 Installing ELK Stack

To set up the ELK stack, follow these steps:

15.1.1 Step 1: Install Elasticsearch

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -
echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-8.x.list
sudo apt update
sudo apt install elasticsearch -y
```

Enable and start the Elasticsearch service:

```
sudo systemctl enable elasticsearch
sudo systemctl start elasticsearch
```

15.1.2 Step 2: Install Logstash

```
sudo apt install logstash -y
```

15.1.3 Step 3: Install Kibana

```
sudo apt install kibana -y
sudo systemctl enable kibana
sudo systemctl start kibana
```

Once installed, Kibana will be accessible at:

```
http://localhost:5601
```

once you are done with all the installation process, now we will send our nvd-cves file to elastic search. for that you may have to get the authorization credentials.

```
curl -u elastic:"wlt8i+2TdnvX0dn-EBES" -X POST
      "https://localhost:9200/nvd_cve_index/_bulk"
      -H "Content-Type: application/json" --data
      -binary @/home/musharaf-misp-admin/
      nvd_cve_bulk.json -k
```

note : replace this "wlt8i+2TdnvX0dn-EBES" with your actual password of elastic

upon successful completion you should see something like this

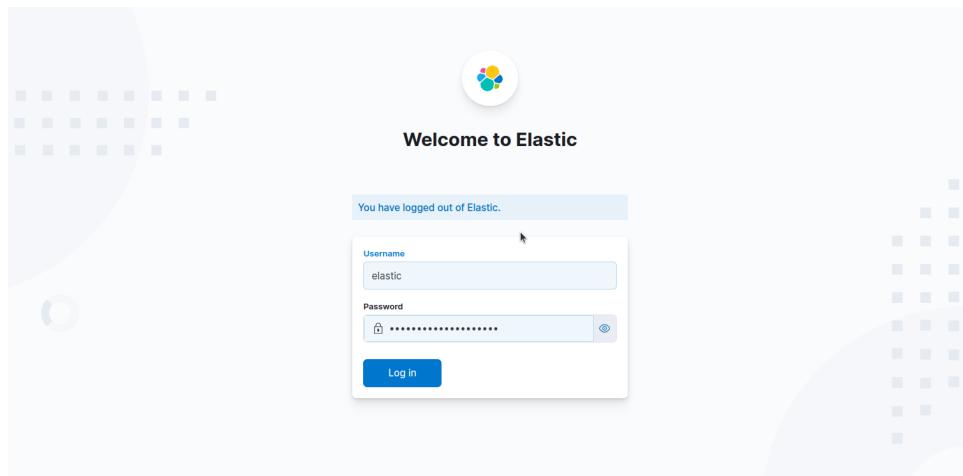
so with the help of above command we are able to send data into elastic search in required bulk format.

similarly follow the exact steps for misp cves file that is in stix2 format using the same command but only replacing the file name.

NOTE: you can also use log stash for sending files to elastic search since we are dealing with smaller files we will use curl in our terminal

15.2 how ELASTICSEARCH works for correlation

- step1 : once you Open Kibana (<http://localhost:5601>). (you have to sign up for your authorization credentials)



- once you sign up you should see something like this as your dashboard

The screenshot shows the Elastic Home dashboard. At the top, there's a navigation bar with a search bar and some icons. Below it is a section titled "Welcome home" with four cards:

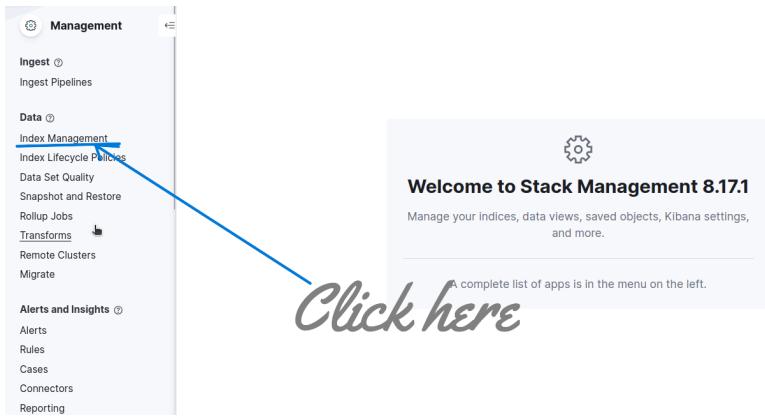
- Elasticsearch**: Create search experiences with a refined set of APIs and tools.
- Observability**: Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.
- Security**: Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.
- Analytics**: Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Below these cards, there's a section titled "Get started by adding integrations" with a brief description and a "Move to Elastic Cloud" button. To the right, there's a "Try managed Elastic" section with a "Move to Elastic Cloud" button.

- next step

The screenshot shows the same Elastic Home dashboard as before, but with a red arrow pointing to the "Management" link in the sidebar. The sidebar also includes links for Findings, Cases, Timelines, Intelligence, Explore, Manage, Dev Tools, Integrations, Fleet, Osquery, Stack Monitoring, and Stack Management. A blue button at the bottom of the sidebar says "+ Add integrations". Overlaid on the dashboard are large yellow and red text instructions: "1. click here and then scroll down" pointing to the sidebar, and "2. click on management" pointing to the "Management" link in the sidebar.

- next



- next

Name	Health	Status	Primaries	Replicas	Documents...	Storage size	Data stream
misp_cves	yellow	open	1	1	191	42.75kb	
nvd_cve_index	yellow	open	1	1	2,000	8.86mb	

Here you can see our two files, one containing misp cves and another containing NVD cves

15.3 Creating data views

1. first

2. second

3. Now comes the important step

(a) Open Data View Management

- Click on the ”Create data view” button.

(b) Enter Data View Details

- **Name:** Set a name for the data view, e.g., `misp-cves`.
- **Index Pattern:** Use `misp*` to match all indices that start with `misp`.
- Ensure the matching index appears on the right under ”**Matching sources**”.

(c) Select Timestamp Field (If Available)

- If the index has a timestamp field, select it.
- If no timestamp field is found (as seen in Figure ??), you can proceed without one.

(d) Save the Data View

(e) Repeat same steps for NVD-cves

- Click ”**Save data view to Kibana**” to finalize the setup.

4. once you are done you will be able to find the cves in any of the folder below for nvd cves in data view they are in id folder like this.

The screenshot shows the Kibana Data View interface for the 'nvd_cves' index. The left sidebar displays available fields: 'references.tags', 'references.url', 'sourceIdentifier', 'vendorComments.comment', 'VendorComments.lastModified', 'vendorComments.organization', 'vulnStatus', 'weaknesses.description.lang', 'weaknesses.description.value', 'weaknesses.source', and 'weaknesses.type'. Under 'Meta fields', there are '_id', '_ignored', '_index', and '_score'. The main panel shows a list of CVE entries with their descriptions and IDs. For example, CVE-2007-5659 is described as 'ExploitAdd Sep 15, 2022 @ 05:38:00:000 cisaRequiredAction Apply updates per vendor instructions. Flow Vulnerability configurations.nodes.cpeMatch.criteria [cpe:2.3:o:linux:linux_kernel...]'.

5. and for misp cves, CVEs are in name folder

The screenshot shows the Kibana Data View interface for the 'misp_cves' index. The left sidebar displays available fields: 'event_id', 'id', and 'name'. Under 'Meta fields', there are '_id', '_ignored', '_index', and '_score'. The main panel shows a list of CVE entries with their names and IDs. For example, CVE-2012-0158 is listed as 'Top value' with a 4.7% frequency.

15.4 Performing correlation between cves of misp and nvd

The screenshot shows the Kibana Discover interface. The left sidebar has sections for 'Home', 'Recently viewed' (Findings, Cases, Timelines, Intelligence, Explore, Manage), 'Management' (Dev Tools, Integrations, Fleet, Osquery, Stack Monitoring, Stack Management), and 'Management' (Dev Tools). A red arrow points to the 'Dev Tools' link under the 'Management' section. The main panel shows a list of CVE documents with their event IDs, IDs, names, and scores.

Navigating to Dev Tools in Kibana: To access the console in Kibana, go to the **Management** section in the left sidebar and click on **Dev Tools**, as indicated by the arrow.

16 Correlation Queries in Kibana Console

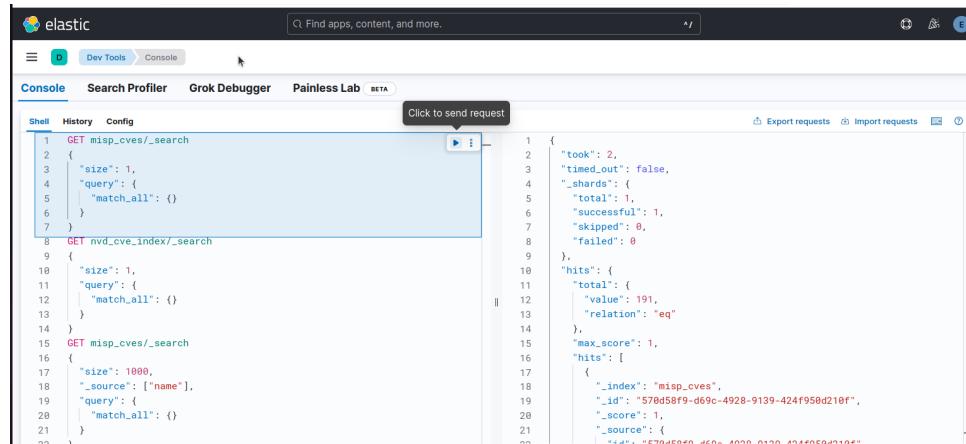
To perform correlation between threat intelligence data from MISP and vulnerability data from NVD, several Elasticsearch queries were executed using Kibana's Dev Tools. These queries help retrieve relevant data for analysis.

16.1 Retrieving Data from MISP and NVD Indices

The following queries fetch data from the `misp_cves` and `nvd_cve_index` indices.

Listing 1: Retrieve sample data from MISP and NVD indices

```
GET misp_cves/_search
{
  "size": 10,
  "query": {
    "match_all": {}
  }
}
```



```
Click to send request
1 GET misp_cves/_search
2 {
3   "size": 10,
4   "query": {
5     "match_all": {}
6   }
7 }
8 GET nvd_cve_index/_search
9 {
10   "size": 1,
11   "query": {
12     "match_all": {}
13   }
14 }
15 GET misp_cves/_search
16 {
17   "size": 1000,
18   "_source": ["name"],
19   "query": {
20     "match_all": {}
21   }
22 }
```

```
GET nvd_cve_index/_search
{
  "size": 1,
  "query": {
    "match_all": {}
  }
}
```

```
1  GET misp_cves/_search
2  {
3    "size": 1,
4    "query": {
5      "match_all": {}
6    }
7  }
8  GET nvd_cve_index/_search
9  {
10   "size": 1,
11   "query": {
12     "match_all": {}
13   }
14 }
15 GET misp_cves/_search
16 {
17   "size": 1000,
18   "_source": ["name"],
19   "query": {
20     "match_all": {}
21   }
22 }
```

Click to send request

```
6   "successful": 1,
7   "skipped": 0,
8   "failed": 0
9 },
10 "hits": {
11   "total": {
12     "value": 2000,
13     "relation": "eq"
14   },
15   "max_score": 1,
16   "hits": [
17     {
18       "_index": "nvd_cve_index",
19       "_id": "CVE-2013-2596",
20       "_score": 1,
21       "_ignored": [
22         "descriptions.value.keyword"
23       ],
24       "_source": {
25         "id": "CVE-2013-2596",
26         "sourceIdentifier": "cve@mitre.org",
27       }
28     }
29   ]
30 }
```

Clear this input Clear this output 200 - OK 92 ms

These queries retrieve a limited number of documents from both indices, ensuring that the data structure and fields are correctly understood before performing correlation.

16.2 Extracting CVE Names from MISP

To extract CVE names from the `misp_cves` index, the following query was executed:

Listing 2: Retrieve CVEs from MISP index

```
GET misp_cves/_search
{
  "size": 1000,
  "_source": ["name"],
  "query": {
    "match_all": {}
  }
}
```

```

14
15 GET misp_cves/_search
16 {
17   "size": 1000,
18   "_source": ["name"],
19   "query": {
20     "match_all": {}
21   }
22 }
23 GET nvd_cve_index/_search
24 {
25   "size": 100,
26   "query": {
27     "terms": {
28       "id.keyword": [
29         "CVE-2015-1641"
30       ]
31     }
32   }
33 }
34
35

```

This query retrieves up to 1000 CVE from the MISP index while excluding unnecessary fields.

16.3 Filtering NVD Data for a Specific CVE

To check for the presence of a specific CVE (e.g., CVE-2015-1641) in the NVD dataset, the following query was used:

Listing 3: Search for a specific CVE in NVD

```

GET nvd_cve_index/_search
{
  "size": 100,
  "query": {
    "terms": {
      "id.keyword": [
        "CVE-2015-1641"
      ]
    }
  }
}

```

This query searches the NVD index for entries with the specified CVE ID.

```

Shell History Config
14
15 GET misp_cves/_search
16 {
17   "size": 1000,
18   "_source": ["name"],
19   "query": {
20     "match_all": {}
21   }
22 }
23 GET nvd_cve_index/_search
24 {
25   "size": 100,
26   "query": {
27     "terms": {
28       "id.keyword": [
29         "CVE-2015-1641"
30       ]
31     }
32   }
33 }
34
35

```

Click to send request

200 - OK 81 ms

Analysis of Response:

- "took": 9 - The query execution time was 9 milliseconds.

- "`timed_out`": `false` - The query did not exceed the allowed time limit.
- "`_shards`" - The response shows that 1 shard processed the request successfully without failures.
- "`hits.total.value- "hits.hits" - Contains the retrieved document details.
- "_index": "nvd_cve_index" - The document belongs to the nvd_cve_index dataset.
- "_id": "CVE-2015-1641" - Confirms that the retrieved document corresponds to CVE-2015-1641.
- "_score": 1 - Indicates the relevance score of the document to the search query.`

16.3.1 Conclusion

The query successfully identified that `CVE-2015-1641` exists in the NVD index. This confirms that there is a known vulnerability associated with this identifier, and further details can be extracted for security analysis.

17 correlation without ELK

1. First we use python code in jupyter to fetch the neccassry CVEs for correlation

```
import json

def extract_cves_from_misp(file_path):
    """Extracts CVEs and groups them by their
       event IDs from the MISP JSON file"""
    with open(file_path, "r") as f:
        misp_data = json.load(f)

    event_cve_mapping = {}

    for entry in misp_data:
        event_id = entry.get("event_id", "Unknown Event")
        cve_id = entry.get("name", "Unknown CVE")

        if event_id not in event_cve_mapping:
            event_cve_mapping[event_id] = []

        event_cve_mapping[event_id].append(
            cve_id)

    return event_cve_mapping

#      Load the JSON file and extract CVEs
#      grouped by events
misp_file_path = "/home/musharaf-misp-admin/
    musharaf/all_misp_cves.json" # Path to the
    uploaded file
misp_cve_mapping = extract_cves_from_misp(
    misp_file_path)

#      Print extracted mappings
print("Extracted MISP CVEs grouped by Event ID:
    ")
```

```

for event, cves in misp_cve_mapping.items():
    print(f"\n Event ID: {event}")
    for cve in set(cves): # Using set() to
        remove duplicates
        print(f" - CVE: {cve}")

```

note: replace the file path your actual file path

```

# Load the JSON file and extract CVEs grouped by events
misp_file_path = "/home/musharaf-misp-admin/musharaf/all_misp_cves.json" # Path to the uploaded file
misp_cve_mapping = extract_cves_from_misp(misp_file_path)

# Print extracted mappings
print("Extracted MISP CVEs grouped by Event ID:")
for event, cves in misp_cve_mapping.items():
    print(f"\n Event ID: {event}")
    for cve in set(cves): # Using set() to remove duplicates
        print(f" - CVE: {cve}")

```

Extracted MISP CVEs grouped by Event ID:

- Event ID: 80
 - CVE: CVE-2015-1641
- Event ID: 84
 - CVE: CVE-2015-1770
 - CVE: CVE-2012-1856
 - CVE: CVE-2015-1641
 - CVE: CVE-2012-0158
- Event ID: 91
 - CVE: CVE-2014-6332
- Event ID: 92
 - CVE: CVE-2015-2545
- Event ID: 106

- now I will use nessus scan of my system her for correlation, here will fetch cves from nessus scan file

```

import xml.etree.ElementTree as ET

def extract_cves_cpes_from_nessus(file_path):
    """Extracts CVEs and CPEs from a Nessus
       scan report and groups by host"""
    tree = ET.parse(file_path)
    root = tree.getroot()

    nessus_cve_cpe = {}

    for report_host in root.findall("./ReportHost"):
        host_name = report_host.get("name", "Unknown Host")

        for report_item in report_host.findall("./ReportItem"):
            # Extract CVEs
            cve_list = report_item.find("cve")
            cve_ids = cve_list.text.split(",")

```

```

        if cve_list is not None else []

        # Extract CPE
        cpe_element = report_item.find("cpe")
        cpe = cpe_element.text if
            cpe_element is not None else "Unknown CPE"

        for cve_id in cve_ids:
            if host_name not in
                nessus_cve_cpe:
                    nessus_cve_cpe[host_name] =
                        {}
            if cve_id not in nessus_cve_cpe[host_name]:
                nessus_cve_cpe[host_name][
                    cve_id] = set()

            if cpe != "Unknown CPE":
                nessus_cve_cpe[host_name][
                    cve_id].add(cpe)

    return nessus_cve_cpe

#      Load Nessus file and extract CVEs & CPES
#      grouped by host
nessus_file_path = "/home/musharaf-misp-admin/
    musharaf/misp scan_f20myj.nessus" # Update
    path accordingly
nessus_cve_cpe_mapping =
    extract_cves_cpes_from_nessus(
        nessus_file_path)

#      Print extracted Nessus CVEs and CPES
#      grouped by hosts
print("\n Extracted Nessus CVEs and CPES:")
if nessus_cve_cpe_mapping:
    for host, cve_data in

```

```

        nessus_cve_cpe_mapping.items():
            print(f"\n Host: {host}")
            for cve, cpes in cve_data.items():
                print(f"    {cve}")
                for cpe in cpes:
                    print(f"        - CPE: {cpe}")
else:
    print("      No CVEs found in the Nessus scan
          report!")

```

```

jupyter project Last Checkpoint: 7 minutes ago
File Edit View Run Kernel Settings Help
JupyterLab Trusted Python 3 (ipykernel)
# Extracted Nessus CVEs and CPES:
print("Extracted Nessus CVEs and CPES:")
if nessus_cve_cpe_mapping:
    for host, cve_data in nessus_cve_cpe_mapping.items():
        print(f"\n Host: {host}")
        for cve, cpes in cve_data.items():
            print(f"    {cve}")
            for cpe in cpes:
                print(f"        - CPE: {cpe}")
else:
    print("No CVEs found in the Nessus scan report!")

# Extracted Nessus CVEs and CPES:
Host: 172.31.101.67
    * CVE-2025-23083
    * CPE: cpe:/a:nodejs:node.js
    * CVE-2016-2183
    * CPE: cpe:/a:node-tar_project:node-tar
    * CVE-2016-2183
    * CVE-2009-3129
    * CPE: cpe:/o:canonical:ubuntu_linux:22.04:-:lts
cpe:/o:canonical:ubuntu_linux:23.10
cpe:/o:canonical:ubuntu_linux:24.04:-:lts
p-cpe:/a:canonical:ubuntu_linux:libcjson-dev
p-cpe:/a:canonical:ubuntu_linux:libcjson1
p-cpe:/a:canonical:ubuntu_linux:docker.io
    * CVE-2024-29018
    * CPE: cpe:/o:canonical:ubuntu_linux:18.04:-:lts
cpe:/o:canonical:ubuntu_linux:24.04:-:lts
p-cpe:/a:canonical:ubuntu_linux:docker.io

```

Now once we have got CVEs from both files we will perform correlation

```

def correlate_misp_nessus(misp_data,
                           nessus_data):
    """Correlates CVEs from MISP (Threat Intel)
       and Nessus (Vulnerability Scan)"""
    correlation_results = {}
    common_cves = set()

    # Extracting CVEs from MISP (Flattening event-
    # wise mapping)
    misp_cve_list = set()
    for event_cves in misp_data.values():
        misp_cve_list.update(event_cves)

    # Extracting CVEs from Nessus (Flattening host
    # -wise mapping)
    nessus_cve_list = set()
    nessus_cpe_map = {} # To store CPES per CVE

```

```

for host, cve_data in nessus_data.items():
    for cve, cpes in cve_data.items():
        nessus_cve_list.add(cve)
        if cve not in nessus_cpe_map:
            nessus_cpe_map[cve] = set()
        nessus_cpe_map[cve].update(cpes)

# Find common CVEs
common_cves = misp_cve_list & nessus_cve_list

if common_cves:
    for cve in common_cves:
        correlation_results[cve] = {
            "misp_events": [event for event,
                            cves in misp_data.items() if cve
                            in cves],
            "nessus_hosts": [host for host,
                            cve_data in nessus_data.items()
                            if cve in cve_data],
            "nessus_cpes": list(nessus_cpe_map
                                .get(cve, set())) # Get
                                correlated CPEs
        }

return correlation_results, misp_cve_list,
       nessus_cve_list, common_cves

# Perform correlation
correlation_results, misp_cves, nessus_cves,
common_cves = correlate_misp_nessus(
    misp_cve_mapping, nessus_cve_cpe_mapping)

# Print correlation results
print("\n Correlation Between MISP Threat Intel &
      Nessus Scan:")

if common_cves:
    for cve, data in correlation_results.items():

```

```

        print(f"\n CVE: {cve}")
        print("      MISP Events Containing This CVE
              : ", data["misp_events"])
        print("      Nessus Hosts Affected:", data[
              "nessus_hosts"])
        print("      CPEs Found in Nessus:", data[
              "nessus_cpes"] if data["nessus_cpes"]
              else "None")
    else:
        print("\n      No Matching CVEs Found Between
              MISP and Nessus!")
    print("\n MISP CVEs:", sorted(misp_cves))
    print("\n Nessus CVEs:", sorted(nessus_cves))

```

```

if common_cves:
    for cve, data in correlation_results.items():
        print(f"\n + CVE: {cve}")
        print(" - 🔍 MISP Events Containing This CVE:", data["misp_events"])
        print(" - 🔍 Nessus Hosts Affected:", data["nessus_hosts"])
        print(" - 🔍 CPEs Found in Nessus:", data["nessus_cpes"] if data["nessus_cpes"] else "None")
else:
    print("\n X No Matching CVEs Found Between MISP and Nessus!")
    print("\n 🔍 MISP CVEs:", sorted(misp_cves))
    print("\n 🔍 Nessus CVEs:", sorted(nessus_cves))

# Correlation Between MISP Threat Intel & Nessus Scan:
+ CVE: CVE-2009-3129
  🔍 MISP Events Containing This CVE: ['294']
  🔍 Nessus Hosts Affected: ['172.31.101.67']
  🔍 CPEs Found in Nessus: ['cpe:/o:canonical:ubuntu_linux:22.04:-:lts\nfce:/o:canonical:ubuntu_linux:23.10\nfce:/o:canonical:ubuntu_linu
x:24.04:-:lts\nfce:/a:canonical:ubuntu_linux:lib cJSON-dev\nnp-cpe:/a:canonical:ubuntu_linux:lib cJSON1']

[ ]:
[ ]:

```

18 Detailed Project Repository without using elk

If you find hard to follow these python codes here you can use my github repository for the same: MISP and Nessus Scan Correlation (GitHub)