# MISP TRAINING: MISP DEPLOYMENT AND INTEGRATION

CIRCL / TEAM MISP PROJECT

HTTP://www.misp-project.org/ Twitter: @MISPProject

**MISP PROJECT** 



MISP Training: MISP Deployment and Integration

MISP TRAINING: MISP DEPLOYMENT AND INTEGRATION

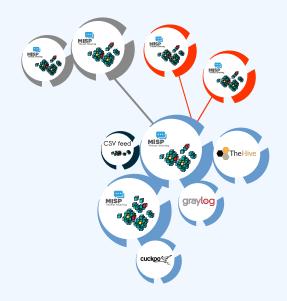
TAM MISP PROJECT

| WWW.MISP-PROJECT.ORG |
R: @MISPPROJECT

ROJECT

| Threat Sharin

## A COMMON INTEGRATION



MISP Training: MISP Deployment and Integration

└─A Common Integration



#### RECOMMENDED MISP SETUP

- Provisioning your MISP infrastructure depends heavily on the **number of attributes/events** (whether your dataset is below or above 50 million attributes).
- Number of MISP instances and the overall design depends on the following factors:
  - ► Is your community private? Are you gathering MISP events from other communities? Are you **publishing events to external** (trusted/untrusted) communities.
  - ► Do you plan to have **automatic tools** (e.g. sandbox analysis or low-value information needing correlation or an analyst workbench) feeding MISP?

MISP Training: MISP Deployment and Integration

2022-09-13

-Recommended MISP Setup

MMENDED MISP SETUP

 Provisioning your MISP infrastructure depends heavily on the number of attributes/events (whether your dataset is

 Number of MISP instances and the overall design deper on the following factors:

n the following factors:

➤ Is your community private? Are you gathering MISP eve from other communities? Are you publishing events to

external (trusted/untrusted) communities.

> Do you plan to have automatic tools (e.g. sandbox analy low-value information needing correlation or an analys

pian to have automatic tools (e.g. sandbox analysis of use information needing correlation or an analyst ench) feeding MISP?

#### **VENDORS AND FORMATS**

- There is a jungle of formats with some vendors having little to no interest in keeping their users autonomous.
- Attacks and threats require a dynamic format to be efficiently shared (e.g. from financial indicators to personal information).
- Review your current list of formats/vendors to ensure a limited loss of information, especially when exporting from MISP to other formats (e.g. STIX not supporting financial indicators or taxonomies/galaxies).

MISP Training: MISP Deployment and Integration

2022-09-13

└─Vendors and Formats

IDORS AND FORMATS

There is a jungle of formats with some vendors having little to no interest in keeping their users autonomous.
Attacks and threats require a dynamic format to be efficiently shared (e.g. from financial indicators to personal

> view your current list of formats/vendors to ensure a itted loss of information, especially when exporting fror 5P to other formats (e.g. STDX not supporting financial icators or taxonomies/galaxies).

#### USE CASE: NORMALIZING OSINT AND PRIVATE FEEDS

- Normalizing external input and feed into MISP (e.g. feed importer).
- Comparing feeds before import (how many similarities? false-positives?).
- Evaluating quality of information before import (warning-list lookup at feed evaluation).

MISP Training: MISP Deployment and Integration

–Use case: Normalizing OSINT and Private Feeds Normalizing external input and feed into MISP (e.g. feed

importer).

false-positives?).

sluating quality of information before import (warning-l okup at feed evaluation).

#### CONNECTING DEVICES AND TOOLS TO MISP

- One of the main goals of MISP is to feed protective or detection tools with data
  - ► IDSes / IPSes (e.g. Suricata, Bro, Snort format as included in Cisco products)
  - ► SIEMs (e.g. CEF, CSV or real-time ZMQ pub-sub or Sigma)
  - ► Host scanners (e.g. OpenIOC, STIX, yara rule-set, CSV)
  - ► Various analysis tools (e.g. Maltego)
  - ► DNS policies (e.g. RPZ)
- Various ways of exporting this data (downloads of the selected data, full exports, APIs)
- The idea was to leave the selection process of the subset of data to be pushed to these up to the user using APIs.

MISP Training: MISP Deployment and Integration

-Connecting Devices and Tools to MISP

- m The idea was to leave the selection process of the subset

#### SIEM AND MISP INTEGRATION

- SIEMs and MISP can be integrated with different techniques depending on the processes at your SOC or IR:
  - ► Pulling events (via the API) or indicator lists at **regular intervals** in a given time frame to perform lookups.
  - ► Subscribing to the MISP ZMQ **pub-sub channel** to directly get the published events and use these in a lookup process.
  - ► **Lookup expansion module** in MISP towards the SIEM to have a direct view of the attributes matched against the SIEM.
- The above options can be combined, depending on your organisation or requirements to increase coverage and detection.

MISP Training: MISP Deployment and Integration

2022-09-13

-SIEM and MISP Integration

ND MISP INTEGRATION

SIEMs and MISP can be integrated with different technique depending on the processes at your SOC or IR:

 Pulling events (via the API) or indicator lists at regular intervals in a given time frame to perform lookups.
 Subscribing to the MISP ZMO pub-sub channel to directly

the published events and use these in a lookup process.

Lookup expansion module in MISP towards the SIEM to h

The above options can be combined, depending on your organisation or requirements to increase coverage an detection

#### ZMQ INTEGRATION: MISP-DASHBOARD

- A dashboard showing live data and statistics from the ZMQ pub-sub of one or more MISP instances.
- Building **low-latency software** by consuming pub-sub channel provides significant advantages over standard API use.
- Process information in **real-time** when it's updated, created, published or gathered in MISP.
- Demo!

MISP Training: MISP Deployment and Integration

-ZMQ integration: misp-dashboard

A dashboard drowing live data and statistics from the ZMQ pub-sho of one or more MSP instances.
 Building lear-beings orbinare by consuming pub-sub channel provides dignificant advantages over standard API stat.

# NEW INTEGRATIONS: IR AND THREAT HUNTING USING MISP

- Close co-operation with **the Hive project** for IR
  - ► Interact with MISP directly from the Hive
  - ► Use both the MISP modules and the **Cortex** analysers in MISP or the Hive directly
- Using MISP to support your threat hunting via **McAfee**OpenDXL
- (https://securingtomorrow.mcafee.com/business/ optimize-operations/ expanding-automated-threat-hunting-response-open-

MISP Training: MISP Deployment and Integration

-New integrations: IR and threat hunting using -

W INTEGRATIONS: IR AND THREAT HUNTING USING SP

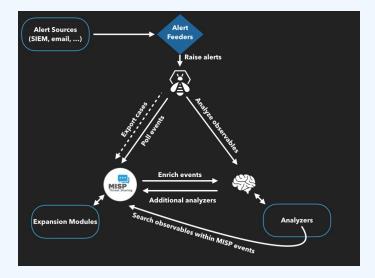
- peration with the Hive project for IR
- Use both the MISP modules and the Cortex analy:
- Using MISP to support your threat hunting via McAfee
   OpenDXI
- OpenDXL

  (https://securingtomorrow.mcafee.com/busine

ptimize-operations/ xpanding-automated-threat-hunting-response-open

8

## THE HIVE INTEGRATION



11

MISP Training: MISP Deployment and Integration

☐ The Hive integration

# REPORTING BACK FROM YOUR DEVICES, TOOLS OR **PROCESSES**

As **Sightings** can be positive, negative or even based on expiration, different use cases are possible:

- **Sightings** allow users to notify a MISP instance about the activities related to an indicator.
- Activities can be from a SIEM (e.g. Splunk lookup validation or **false-positive feedback**), a NIDS or honeypot devices<sup>1</sup>.
- Sighting can affect the API to limit the NIDS exports and improve the NIDS rule-set directly.

MISP Training: MISP Deployment and Integration

-Reporting Back from your Devices, Tools or Processes

https://www.github.com/MISP/misp-sighting-tools

-Q&A

- info@circl.lu (if you want to join the CIRCL MISP sharing community)
- https://github.com/MISP/http://www.misp-project.org/
- We welcome any contributions to the project, be it pull requests, ideas, github issues,...