# **MISP DEPLOYMENT**

Some basic guidelines

CIRCL / TEAM MISP PROJECT



13TH ENISA-EC3 WORKSHOP

MISP Deployment

CIRCL / TEAM MISP PROJECT

MISP Treat Sharing 13TH ENISA-EC3 WORKSHO

## MISP DEPLOYMENT CONSIDERATIONS

MISP DEPLOYMENT CONSIDERATIONS

MISP Deployment

└─MISP deployment considerations

Deployment types
 Distro choice
 Hardware specs
 Authentication
 Other considerations - settings, gotchas

# Deployment types

**Distro** choice

Hardware specs

Authentication

Other considerations - settings, gotchas

## **DEPLOYMENT TYPES**

## Native install

- Manual
- One-liner script INSTALL.sh: https://github.com/MISP/MISP/tree/2.4/INSTALL

■ MISP VM:

- https://www.circl.lu/misp-images/latest/
- Docker: https://github.com/MISP/misp-docker
- RPM maintained by amuehlem: https://github.com/misp/misp-rpm
- Cloud provider images:
  - https://github.com/MISP/misp-cloud
- LXC images via misp-airgap: https://github.com/MISP/misp-airgap/

MISP Deployment

3

2024-

■ Native install ► Manual

 Manual evolve. TMCTAL.cb/ https://twolve.tml/star/MISP/tree/2.c/INSTALL
 MSP VM https://www.circllu/misp-images/latest/
 Docken https://github.com/MISP/misp-docker
 RPM maintained by anuchlem. https://github.com/misp/misp-rpm
 Cloud provide images:

 LXC images via misp-airgap: https://github.com/MISP/misp-airgap/

#### **DOCKER OPTIONS**

MISP Deployment

3

2024-10

L Docker options

DOCKER OPTIONS

There are several MISP Docker installations available.
 The official MISP Docker installation is maintained by ostef and and can be found at https://github.com/RISP/misp-docker.
 The official MISP Docker image also includes one for the MISP modules.

- There are several MISP Docker installations available.
- The official MISP Docker installation is maintained by ostefano and can be found at https://github.com/MISP/misp-docker.
- The official MISP Docker image also includes one for the MISP modules.

#### **DISTRO OPTIONS**

**MISP** Deployment

8

-10

2024

#### └─Distro options

DISTRO OPTIONS

- B Ubuntu 22.04 (20.04 will also work)
- Our target platform
   Our Climent
- Our citarget
   Use this unless you are absolutely forced n
- This is the platform we can support you with?
- CentOS 7
  Annoying to operate
- Jumoying to operate
   Less tested, though used by many
- CentOS is dead. Consider other opt
   RHEL 7
- RHEL 7
- Same annoyance as centos in general.
   We test against CentOS in general, some assembly may required

# Ubuntu 22.04 (20.04 will also work)

- Our target platform
- Our CI target
- Use this unless you are absolutely forced not to
- This is the platform we can support you with!

#### CentOS 7

- Annoying to operate
- Less tested, though used by many
- CentOS is dead. Consider other options

#### RHEL 7

- Same annoyance as CentOS in general
- We test against CentOS in general, some assembly may be required

MISP Deployment

10-02

2024

No firm recommendations, it's highly usage dependent
 It's better to go a bit over what you need than under
 SDS are massively beneficial
 Let's look at what affects specs and some sample
 configurations

- No firm recommendations, it's highly usage dependent
- It's better to go a bit over what you need than under
- **SSDs** are massively beneficial
- Let's look at what affects specs and some sample configurations

**MISP Deployment** 

3

9

2024-

Hardware considerations

- What are the factors that can impact my performance?
   Clustering of the data (how many datapoints / event?) (RAM, disk sneed)
- correlation (RAM, disk speed, disk space)
   Consider blocking overthy correlating values from doing so
- Consider blocking overtly correlating values from doing s
   Feed ingestion strategy is crucial
- Over-contextualisation (RAM, disk speed)
   Totilation difference in the speed instead of each attribute
- Tag/attach galaxies to the event instead of each attribute v possible

- What are the factors that can impact my performance?
  - Clustering of the data (how many datapoints / event?) (RAM, disk speed)
  - Correlation (RAM, disk speed, disk space)
    - Consider blocking overtly correlating values from doing so
    - Feed ingestion strategy is crucial
  - Over-contextualisation (RAM, disk speed)
    - Tag/attach galaxies to the event instead of each attribute when possible

#### HARDWARE CONSIDERATIONS - CONTINUES

**MISP** Deployment

10-02

2024-

Hardware considerations - continues

- What are the factors that can impact my performance?
   Number of users that are active at any given time (RAM, CPU
- disk speed)
- API users especially with heavy searches (substring searche for example) (RAM, CPU, Disk speed)

#### What are the factors that can impact my performance?

- Number of users that are active at any given time (RAM, CPU, disk speed)
- Logging strategy (Disk space)
- API users especially with heavy searches (substring searches for example) (RAM, CPU, Disk speed)

#### HARDWARE CONSIDERATIONS - CONTINUES

**MISP** Deployment

3

2024-10

Hardware considerations - continues

- What are the factors that generally do NOT impact my
- performance as much as expected?
- Warningist usage
   Number of raw attributes on the instance
- Number of sync connections / recurring syncs (with measured)

roots reading on the automation avalog

# ■ What are the factors that generally do **NOT** impact my performance as much as expected?

- ► Warninglist usage
- Number of raw attributes on the instance
- Number of sync connections / recurring syncs (with measure)
- Tools feeding off the automation channels (ZMQ, kafka, syslog)

#### AUTHENTICATION OPTIONS

**MISP** Deployment

8

2024-10

Authentication options

Username / password is the default
Some built in modules by 3rd parties (LDAP, Shibboleth,
x509, OpenID, Azure Active Directory)
CustomAuth system for more flexibility
Additionally, consider Email OTP

#### Username/password is the default

- Some built in modules by 3rd parties (LDAP, Shibboleth, x509, OpenID, Azure Active Directory)
- CustomAuth system for more flexibility
- Additionally, consider Email OTP

#### OTHER CONSIDERATIONS - TUNING

**MISP Deployment** 

8

2024-10

└─Other considerations - tuning

- PHP tuning
   Maximum memory usage (per process)
- Maximum memory usage (per process,
   Timeout settings
- Consider setting it per role!
   Backsmund processes are exempt
- MySQL: key buffer size is important
- Generally, tune for few heavy requests rather than many light ones

- PHP tuning
  - Maximum memory usage (per process)
  - Timeout settings
  - Consider setting it per role!
  - Background processes are exempt
- MySQL: key buffer size is important
- Generally, tune for few heavy requests rather than many light ones

#### **OTHER CONSIDERATIONS - HIGH AVAILABILITY**

**MISP Deployment** 

8

-10

2024-

—Other considerations - high availability

# Clustering Load balanced spache servers with NLSP Replicating / mirrored database backends Careful about session pinning Attachment storage can be abstracted / network attached

An example implementation for AWS

- Clustering
  - Load balanced apache servers with MISP
  - Replicating / mirrored database backends
- Careful about session pinning
- Attachment storage can be abstracted / network attached
- An example implementation for AWS https://github.com/oxtf/HAMISPA