MISP Future

What to expect in the next few months

Team CIRCL

MISP Training @ CONCORDIA
20191017

We have a massive rework of the MISP internals planned

- Upgrade to a more **modern version of the framework** (CakePHP 3.x paving the way to 4.x)
- Move to a more **modern UI** (Bootstrap 4 based)
- Good moment to rid ourselves of a LOT of **legacy** baggage
- Some of the work has already started behind the scenes

Some things that will change

- First time we’ll have a **manual upgrade** to a new version of MISP since 2015
    - This means you’ll get an upgrade script that needs to be executed, MISP made unavailable during the upgrade
    - **All sync / modern APIs will be compatible between the old/new versions**
- Raising the requirements of the supported language versions (**PHP 7.2+, Python 3.6+**)
- CakePHP 3.x’s backend is quite different, so we’ll use the opportunity for a refactor

What this will mean for users

- Leaner and **more performant** MISP
- Cuttig down on a lot of long **deprecated** baggage
- Sleeker UI
- One of our planned improvements is to be able to run MISP in two separate modes of operation (**endpoint vs sharing hub**)
  - MISP is built as a shared use system from the ground up
  - We see many use cases where it's used as an endpoint/internal tool
  - We want to reduce the burden on these installations

The current plan for the whole process

- Tying off loose ends
- Preparation phase
- Transition phase
- Post release support

Tying off loose ends

- We are currently busy with finishing off a set of features that are high priority first
  - **"Zoidberg"**
  - first/last seen with time based correlation
  - Modular **feed parsing**
  - Markdown based **reports** attached to events
  - Working through a stockpile of **pull requests**

Preparation phase

- This phase can be handled in **parallel to other tasks**, so generally business as usual
- We welcome community members to join us for this effort
- Simplify a lot of the backend code, switch to a light-weight middleware that interfaces with both cake 2.x/3.x and that makes building new functionalities simpler with MISP in mind
- get rid of the inconsistent current view system and move to generated views (we have already migrated parts of the UI over the past few months)
- A good moment to re-evaluate some decisions we've made and improve the consistency / simplicity of the code-base

Transition phase

- This is where the **real transition will happen**, we want to move our ORM and UI generators to the new framework
- The preparation phase's output is what should make this a quick transition
- During this phase we will halt the development of new features
- Two branches of MISP in parallel, 2.4 will enter bug fix only mode
- We estimate this phase to be rather short, our plan is to try to cram it in about 1-2 month

Post release support

- We will **keep supporting the old version of MISP** for a short duration after the release
- Two MISP versions operational in parallel
- MISP 2.4 will not receive any new features any longer and will be on **life support**

Other new things planned in upcoming releases

- As part of the **VARIOT** project, add the ability to export feeds in MISP and publish them to **open data** directories
- Work has begun on the next big leap for the feed system: working with feed providers to have their offerings directly available through MISP
- The system incorporated for the decaying of indicators has been a rapid success - thanks to all the feedback we will be incorporating a host of changes
- We are evaluating models to offer professional support for those users that require it

Cerebrate

- Another **OSS tool** meant to help us build organisation registries
- Communities can run centralised installations and/or use the one provided by the misp-project
- Opt-in system for organisations, communities
- Repositories of signing keys for event signing
- Add a list of MISP instances to your cerebrate's **brood**
- Create sync requests to **simplify the process of interconnecting with trusted peers**
- Link up trusted Cerebrates to **join a swarm with your brood**