VISUALISE ALL THE THINGS
BUILDING DASHBOARD WIDGETS FOR MISP

CIRCL / Team MISP Project

HTTP://WWW.MISP-PROJECT.ORG/
TWITTER: @MISPProject

MISP Project

MISP
Threat Sharing

VISUALISE ALL THE THINGS

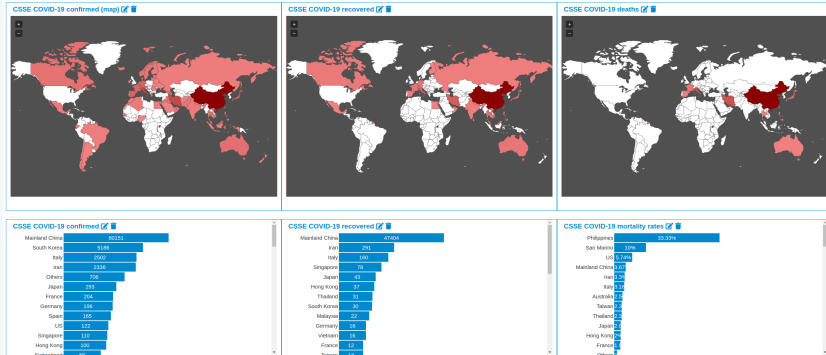## BUILDING DASHBOARD WIDGETS FOR MISP

CIRCL / TEAM MISP PROJECT

HTTP://WWW.MISP-PROJECT.ORG/
TWITTER: @MISPPROJECT

MISP PROJECT

MISP
Threat Sharing

- User configurable simple dashboard interface
- **Visualise**, **aggregate** and **track** data important to you
- Brand new feature, still undergoing reworks

Visualise all the things

Dashboard in MISP

Dashboard in MISP

- User configurable simple dashboard interface
- **Visualise**, **aggregate** and **track** data important to you
- Brand new feature, still undergoing reworks

- **Backend** for the widget, full access to all MISP internals
- **Load, convert, format** to be represented via view widgets
- **Widget metadata** - size, name, description, behaviours
- Only main function required to be implemented: **handler()**
- Optional: **checkPermissions() for ACL**
- Accepts **user configuration** for which a template can be provided
- Located in /var/www/MISP/app/Lib/Dashboard/
- Custom widgets can be placed in /var/www/MISP/app/Lib/Dashboard/Custom/

Visualise all the things

2022-09-13

└─The internals of awidget

- View files are included by default and reusable
- Currently we have a small but growing list of views
  - ▶ BarChart
  - ▶ SimpleList
  - ▶ WorldMap
- Converts the data passed by the Widget logic to HTML
- Located in /var/www/MISP/view/Elements/dashboard/Widgets/

- Widgets can additionally be tied to certain **behaviours**:
  - ▶ Caching
    - Executions of the widget logic are cached
    - **Separate caches for each organisation in addition to site admins**
    - Cache duration is controlled by the widget logic
  - ▶ Refresh
    - Widgets can be set to refresh after x seconds
  - ▶ Both of these should be used with special care in regards to the use of **system resources**

- Let's start with a skeleton
- Create /var/www/MISP/app/Lib/Dashboard/Custom/WhoamiWidget.php
- MISP will parse anything ending with Widget.php in this directory

Exercise module: simple Whoami

```php
1  <?php
2  class MispWhoamiWidget
3  {
4    public $title = 'Whoami';
5    public $render = 'SimpleList';
6    public $width = 2;
7    public $height = 2;
8    public $params = array();
9    public $description = 'Shows information about the
         currently logged in user.';
10   public $cacheLifetime = false;
11   public $autoRefreshDelay = 3;
12
13   public function handler($user, $options = array())
14   {
15     $data = array();
16     return $data;
17   }
18 }
```

6

9

- **$title**: The name of the widget
- **$description**: A description of the widget
- **$render**: The view element to use in rendering the widget
- **$width & $height**: Default relative dimensions
- **$params**: Configuration array with explanations for each key
- **$cacheLifetime**: The lifetime of the caches in seconds (false disables it)
- **$autoRefreshDelay**: The time in seconds between each refresh (false disables it)

Visualise all the things

2022-09-13

└─Meta information

The handler

```php
public function handler($user, $options = array())
{
  $this->Log = ClassRegistry::init('Log');
  $entries = $this->Log->find('all', array(
    'recursive' => -1,
    'conditions' => array(
      'action' => 'login', 'user_id' => $user['id']
    ),
    'order' => 'id desc',
    'limit' => 5,
    'fields' => array('created', 'ip')
  ));
  foreach ($entries as &$entry) {
    $entry = $entry['Log']['created'] . ' --- ' .
    (
      empty($entry['Log']['ip']) ?
      'IP not logged' :
      $entry['Log']['ip']
    );
  }
  return array(
    array('title' => 'Email', 'value' => $user['email']),
    array(
      'title' => 'Role', 'value' => $user['Role']['name']
    ),
    array(
      'title' => 'Organisation',
      'value' => $user['Organisation']['name']
    ),
    array(
      'title' => 'IP', 'value' => $_SERVER['REMOTE_ADDR']
    ),
    array('title' => 'Last logins', 'value' => $entries)
  );
}
```

2022-09-13

Visualise all the things

└─The handler

Whoami ✏️ 🗑️

Email: admin@admin.test
Role: admin
Organisation: ORGNAME
IP: ::1
Last logins:
2020-03-05 06:50:46 --- ::1
2020-03-04 21:35:15 --- IP not logged
2020-03-04 09:34:44 --- IP not logged
2020-03-03 16:58:35 --- IP not logged
2020-03-03 06:49:10 --- IP not logged