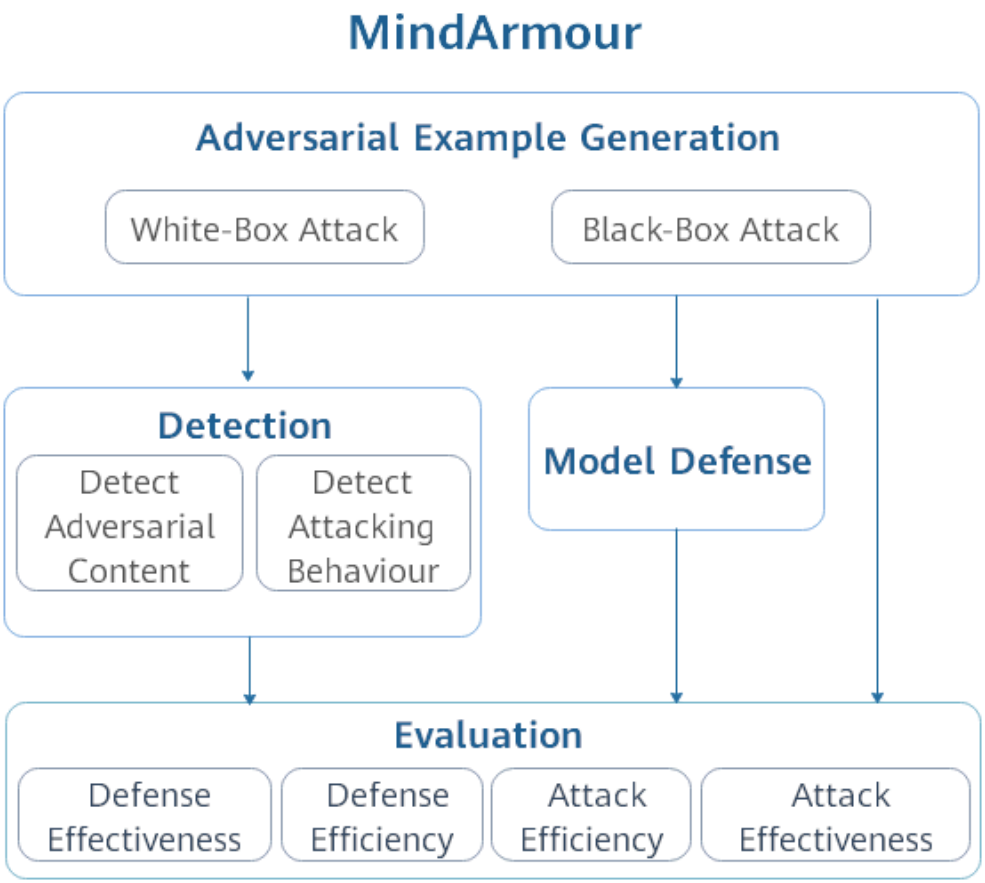
# MindArmour



## What is MindArmour

A tool box for MindSpore users to enhance model security and trustworthiness.

MindArmour is designed for adversarial examples, including four submodule: adversarial examples generation, adversarial example detection, model defense and evaluation. The architecture is shown as follow:




# Setting up MindArmour

## Dependencies

This library uses MindSpore to accelerate graph computations performed by many machine learning models. Therefore, installing MindSpore is a pre-requisite. All other dependencies are included in `setup.py` .

## Installation

### Installation for development

1. Download source code from Gitee.

```
git clone https://gitee.com/mindspore/mindarmour.git
```

2. Compile and install in MindArmour directory.

```
$ cd mindarmour
$ python setup.py install
```

### `Pip` installation

1. Download whl package from MindSpore website, then run the following command:

```
pip install mindarmour-{version}-cp37-cp37m-linux_{arch}.whl
```

2. Successfully installed, if there is no error message such as `No module named 'mindarmour'` when execute the following command:

```
python -c 'import mindarmour'
```

## Docs

Guidance on installation, tutorials, API, see our User Documentation.

## Community

- MindSpore Slack - Ask questions and find answers.

## Contributing

Welcome contributions. See our Contributor Wiki for more details.

## Release Notes

The release notes, see our RELEASE.

## License

Apache License 2.0