FIR

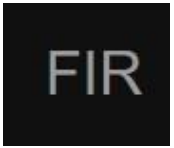
Information Security Inc.

Contents

- About FIR
- Main dependencies
- Testing Environment
- Installing FIR
- Using FIR
- References

About FIR

- FIR (Fast Incident Response) is an cybersecurity incident management platform designed with agility and speed in mind
- It allows for easy creation, tracking, and reporting of cybersecurity incidents



Main dependencies

- OS: Ubuntu 14.04
- Application layer: Python 2.7 & Django 1.7.6
- Webserver: nginx
- Database: MySQL

Testing Environment

- Rancher OS

```
[root@rancher ~]# cat /etc/*rel*
DISTRIB_ID=RancherOS
DISTRIB_RELEASE=v1.1.0
DISTRIB_DESCRIPTION="RancherOS v1.1.0"
NAME="RancherOS"
VERSION=v1.1.0
ID=rancheros
ID_LIKE=
VERSION_ID=v1.1.0
PRETTY_NAME="RancherOS v1.1.0"
HOME_URL="http://rancher.com/rancher-os/"
SUPPORT_URL="https://forums.rancher.com/c/rancher-os"
BUG_REPORT_URL="https://github.com/rancher/os/issues"
BUILD_ID=
```

Installing FIR

- Downloading and running docker-git-alpine -> can use git in Rancher OS

```
[rancher@rancher ~]$ docker pull bwits/docker-git-alpine
Using default tag: latest
latest: Pulling from bwits/docker-git-alpine
627beaf3eaaf: Pull complete
6aef0dfe98f5: Pull complete
e059211f4a7e: Pull complete
Digest: sha256:fa1c222f51d565e908adb870141a3b1da687f174dab1ef5693792e2cccee1384
Status: Downloaded newer image for bwits/docker-git-alpine:latest
```

Installing FIR

- Add an alias

```
[root@rancher ~]# alias git="docker run -ti --rm -v ${HOME}:/root -v $(pwd):/git bwits/docker-git-alpine"
[root@rancher ~]#
```

Installing FIR

- Clone GitHub repository

Installing FIR

- Build the fir Docker image

```
[root@rancher docker]# docker build -t fir .
Sending build context to Docker daemon 3.072 kB
Step 1/13 : FROM alpine:3.4
3.4: Pulling from library/alpine
49388a8c9c86: Pull complete
Digest: sha256:915b0ffca1d76ac57d83f28d568bcb516b6c274843ea8df7fac4b247440f796b
Status: Downloaded newer image for alpine:3.4
 ---> dc98aa467aa0
Step 2/13 : RUN apk add --update     python     python-dev     py-pip     build-base
m -rf /var/cache/apk/*
 ---> Running in 51bb84ac23e0
fetch http://dl-cdn.alpinelinux.org/alpine/v3.4/main/x86_64/APKINDEX.tar.gz
fetch http://dl-cdn.alpinelinux.org/alpine/v3.4/community/x86_64/APKINDEX.tar.gz
(1/53) Upgrading libcrypto1.0 (1.0.2k-r0 -> 1.0.2m-r0)
(2/53) Upgrading libssl1.0 (1.0.2k-r0 -> 1.0.2m-r0)
(3/53) Installing binutils-libs (2.26-r1)
(4/53) Installing binutils (2.26-r1)
(5/53) Installing gmp (6.1.0-r0)
```

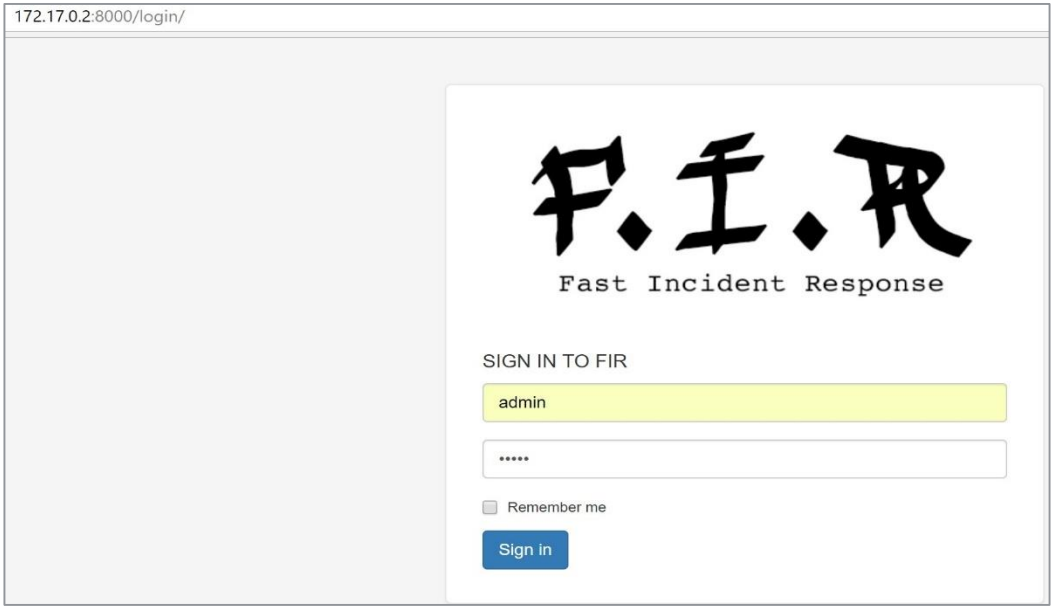
Using FIR

- Running the fir Docker image

```
[root@rancher rancher]# docker run fir
Performing system checks...
```

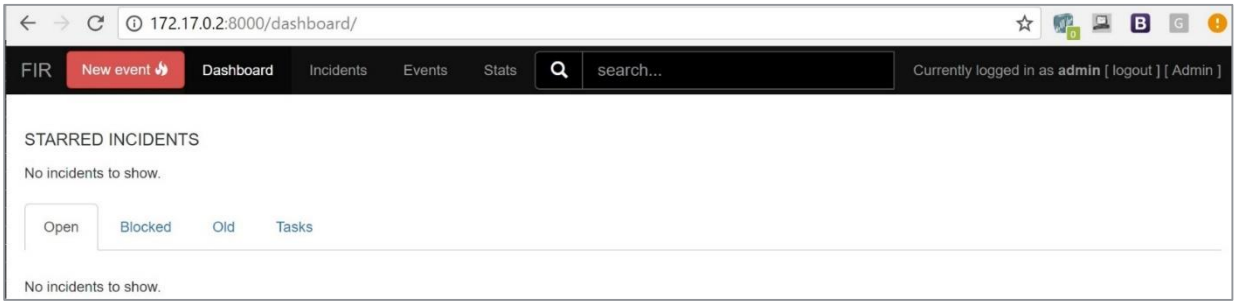
Using FIR

- Accessing Fir -> http://IP:8000, admin:admin



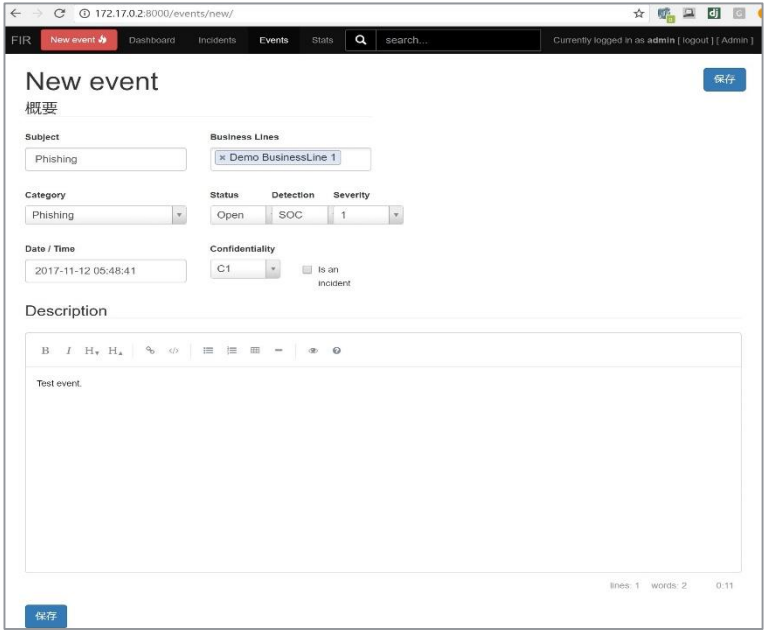
Using FIR

- Accessing Fir -> http://IP:8000, admin:admin



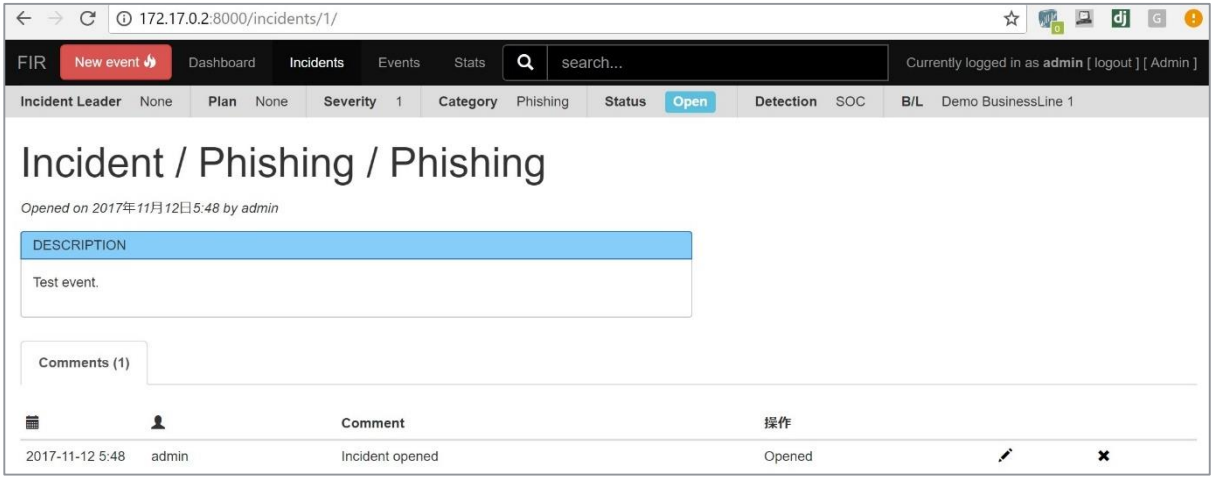
Using FIR

- Creating a new event



Using FIR

- Creating a new event



References

- FIR
https://github.com/certsocietegenerale/FIR

- Rancher OS
http://rancher.com/rancher-os/

- Docker-git-alpine
https://hub.docker.com/r/bwits/docker-git-alpine/