



FIR

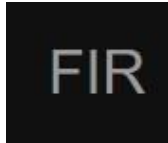
Information Security Inc.

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

```
[root@rancher ~]# git clone https://github.com/certsocietegenerale/FIR.git FIR
Cloning into 'FIR'...
remote: Counting objects: 3131, done.
remote: Total 3131 (delta 0), reused 0 (delta 0), pack-reused 3131
Receiving objects: 100% (3131/3131), 2.09 MiB | 908.00 KiB/s, done.
Resolving deltas: 100% (1658/1658), done.
[root@rancher ~]# cd FIR
[root@rancher FIR]# ls
LICENSE                fir                   fir_artifacts         fir_notifications    fir_threatintel      manage.py
Procfile               fir_abuse            fir_artifacts_enrichment  fir_suggests         fir_todos             requirements.txt
README.md              fir_alerting        fir_calery             fir_plugins          incidents             runtime.txt
docker                 fir_api              fir_email              fir_relations        logs                  uploads
```


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

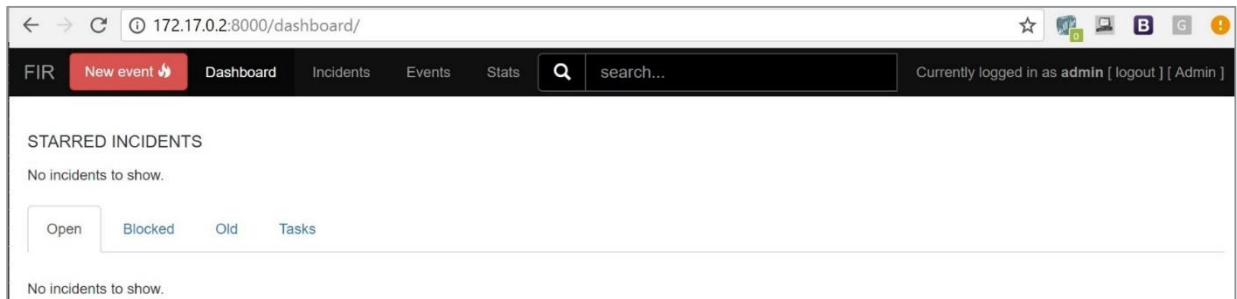
- Accessing Fir -> <http://IP:8000>, admin:admin



The screenshot shows a web browser window with the address bar containing "172.17.0.2:8000/login/". The main content area features a large, stylized logo for "F.I.R." in black, with the text "Fast Incident Response" centered below it. Underneath the logo, the text "SIGN IN TO FIR" is displayed. There are two input fields: the first contains the text "admin" and is highlighted in yellow; the second contains six dots, representing a password field. Below the password field is a checkbox labeled "Remember me" which is currently unchecked. At the bottom of the form is a blue button labeled "Sign In".

Using FIR

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



Using FIR

- Creating a new event

The screenshot shows a web browser window at the URL 172.17.0.2:8000/events/new/. The page title is "New event" and it features a navigation bar with "FIR", "New event", "Dashboard", "Incidents", "Events", and "Stats". A search bar and a user login status "Currently logged in as admin" are also visible.

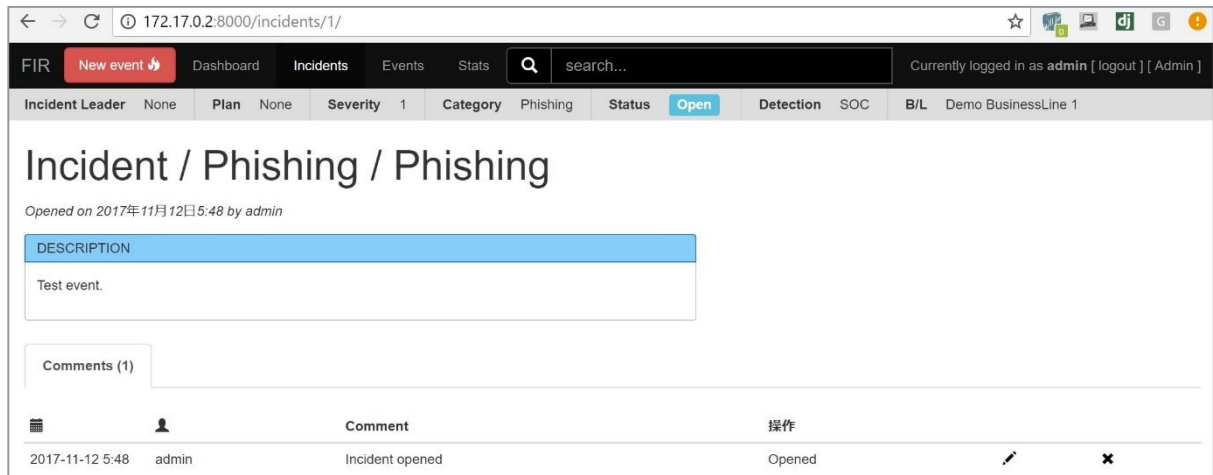
The form is titled "New event" and includes a "概要" (Summary) section with the following fields:

- Subject:** Text input containing "Phishing".
- Business Lines:** Select dropdown containing "Demo BusinessLine 1".
- Category:** Select dropdown containing "Phishing".
- Status:** Select dropdown containing "Open".
- Detection:** Select dropdown containing "SOC".
- Severity:** Select dropdown containing "1".
- Date / Time:** Text input containing "2017-11-12 05:48:41".
- Confidentiality:** Select dropdown containing "C1".
- Is an incident:** A checkbox that is currently unchecked.



Below the summary is a "Description" section with a rich text editor. The editor contains the text "Test event." and a status bar at the bottom right indicating "lines: 1 words: 2 0.11".

Using FIR

- Creating a new event



The screenshot shows a web browser window at the URL 172.17.0.2:8000/incidents/1/. The interface includes a navigation bar with 'FIR' and 'New event' buttons, and a search bar. The main content area displays the incident details for 'Incident / Phishing / Phishing', which was opened on 2017年11月12日 5:48 by admin. A 'DESCRIPTION' field contains the text 'Test event.'. Below this is a 'Comments (1)' section. At the bottom, a table lists the incident details.

📅	👤	Comment	操作
2017-11-12 5:48	admin	Incident opened	Opened  

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/>