FIR

Fast Incident Response

Questions?

Ask them any time

Life before FIR

was not tender

- **6000** line Excel file
- **1 row** per incident, some columns
- **1 cell** for eventual comments
- Stats & reports were generated **with a macro**
- **Single** user (**locked files**)

No tracking

No tracking

No lessons learned

No tracking

No lessons learned

No intel

Alternatives

back in 2012

- We **asked** around…
- **Commercial** solutions → not well adapted
- **RTIR** (Request Tracker mod) → user hostile
- No serious **FOSS** project

No flexibility

No flexibility

Workflow

changes

No flexibility

Workflow

changes

~50% need

coverage

The solution seemed

pretty clear

BUILD!

Tailored environment

No useless features

Near-perfect UX

FIR

in a nutshell

- **Count**, **track**, **manage** cybersec incidents
- More efficient, **less overhead**
- Provides **intelligence** on past incidents
- Generates on-demand **reports** and **statistics**
- Extensible framework
- **Multi-user** (web-based)

Workflow demo

And more...

Demos, demos, demos!

- Artifact collection
- Incident correlation
- Investigation timelines (nuggets)
- Incident attributes
- Statistics

Under the hood

- Web framework - **Django**
- Main language - **Python**
- Sugar coating - **Bootstrap** + **jQuery**
- Bells and whistles - **D3.js**
- Database - **MySQL** (not limited to...)

Similar stuff

MISP - more malware-centric

CRITS - more intel-centric

FIR as in beer

Why open it?

- Figured that **most IR teams** had been confronted to the problem
- **Give** something back to the community
- **Learn** from their contributions

Why open it?

- Figured that **most IR teams** had been confronted to the problem
- **Give** something back to the community
- **Learn** from their contributions

Challenge

Why open it?

- Figured that **most IR teams** had been confronted to the problem
- **Give** something back to the community
- **Learn** from their contributions

Challenge - make it as generic as possible

Not custom enough?

Roll your own, then share

Contributions

- Available on **GitHub** since March
- **Internationalisation** (+ *in le French*)
- Dockerfiles
- New **modules**! (artifacts, articles)
- **7** merged PRs, **42** forks, **29** issues
- Globally **positive** feedback

Roadmap

More work on the TI part

Email ingestion

Web API

Events & hooks

That's all folks!

```
$ git clone https://github.com/certsocietegenerale/FIR
```

Last chance for questions