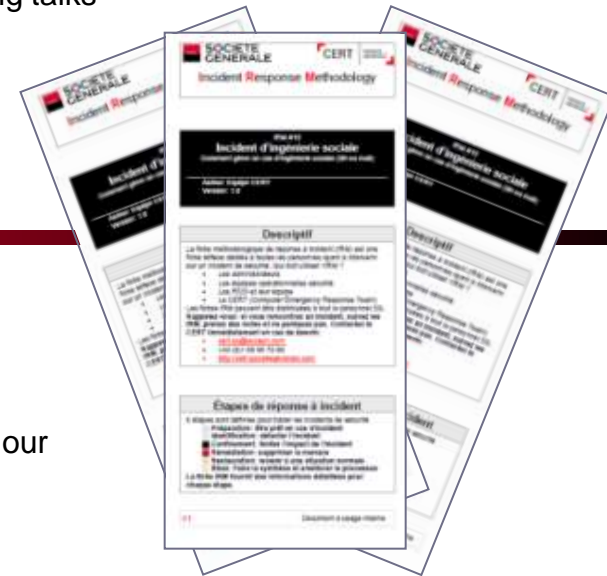


# Incident Response Methodologies



## ▶ What?

▶ Incident response cheatsheets

## ▶ Who?

▶ Dedicated to incident handlers

- Worm infection
- Windows intrusion
- Unix/linux Detection
- DDoS
- Malicious network behaviour
- Defacement
- Insider abuse
- Information leakage
- Smartphone malware
- Social engineering
- Suspicious device

## ▶ Why?

▶ Because it does not exist

## ▶ When?

- ▶ One each week during 12 weeks
- ▶ NOW for FIRST community

## Where?

▶ <http://cert.societegenerale.com/FIRST>

▶ Login : FIRST2011

▶ Password : FIRST23Vienna