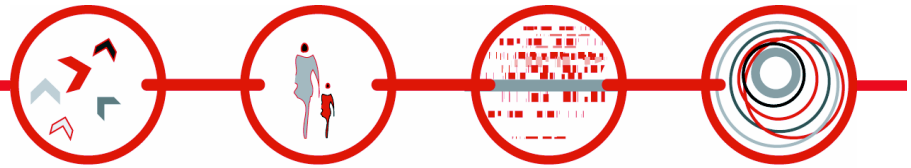
Swedish IT Incident Centre

Establishing a Government CERT from scratch – the Swedish experience

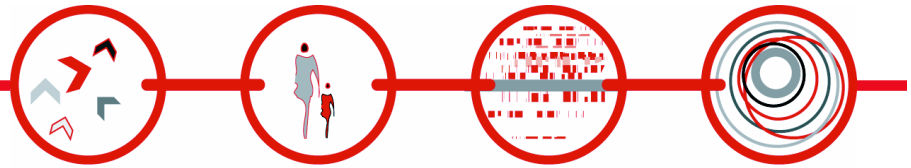
Establishment phase 2003 – 2004

”CERTs in Europe – Lessons Learned and Good Practices”,
Brussels 2005-12-13



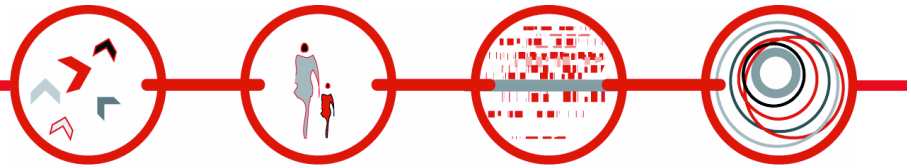
Presentation structure

- Framework
- Assignment
- Basic facts about the resulting Sitic organisation
- Internal vs External view
- What we learnt
  - General remarks
  - For each task in the assignment
  - Hints for budding new organisations



Framework

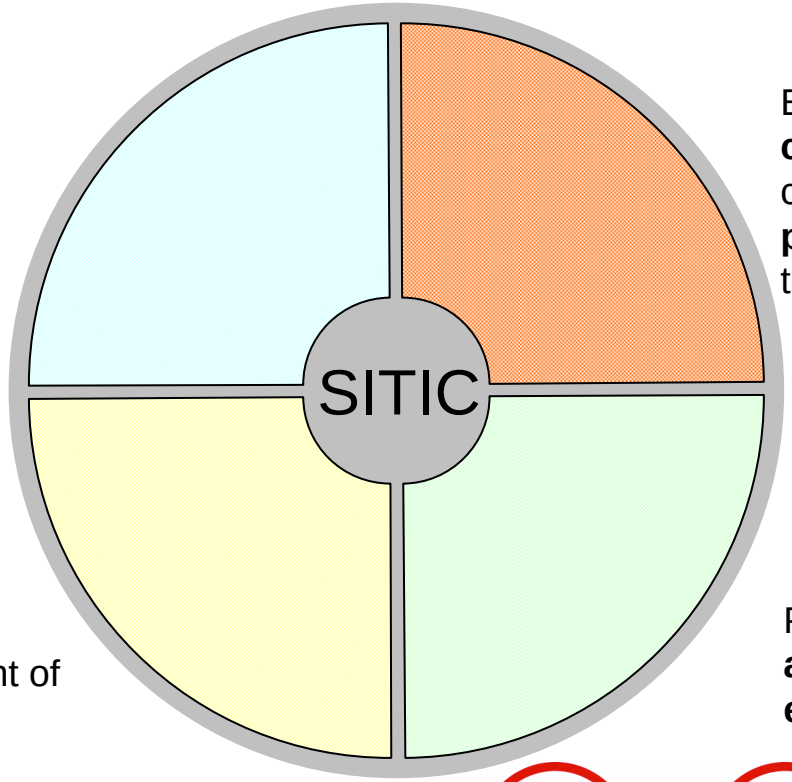
- ”Various” official investigations and reports, ending in a government proposal in 2001
- Official assignment to PTS 2002-05-30
- Operational Jan 2003
- Give an account of achievements and results Dec 2004
  - http://www.pts.se/Archive/Documents/SE/Tvaarsrapport_Sitic_A2_pecr_2004_44_dec04.pdf



PTS assignment

Support society in the efforts against IT incidents by:

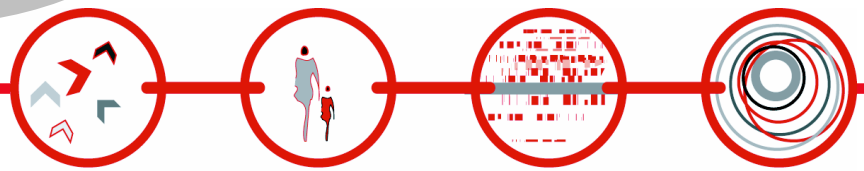
Establishing a system for **information exchange regarding IT incidents** between community organizations and the team



Being able to quickly **communicate information** to the community **regarding new problems**, potentially threatening to IT systems

Aggregate and publish **statistics** as input to continuous improvement of the preventive work

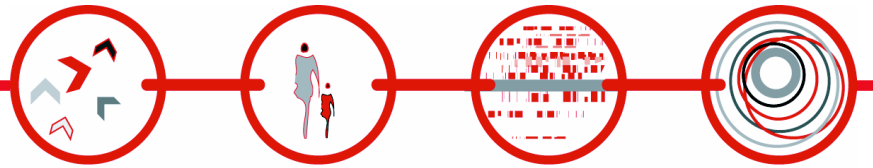
Providing information and **advice regarding preventive efforts**



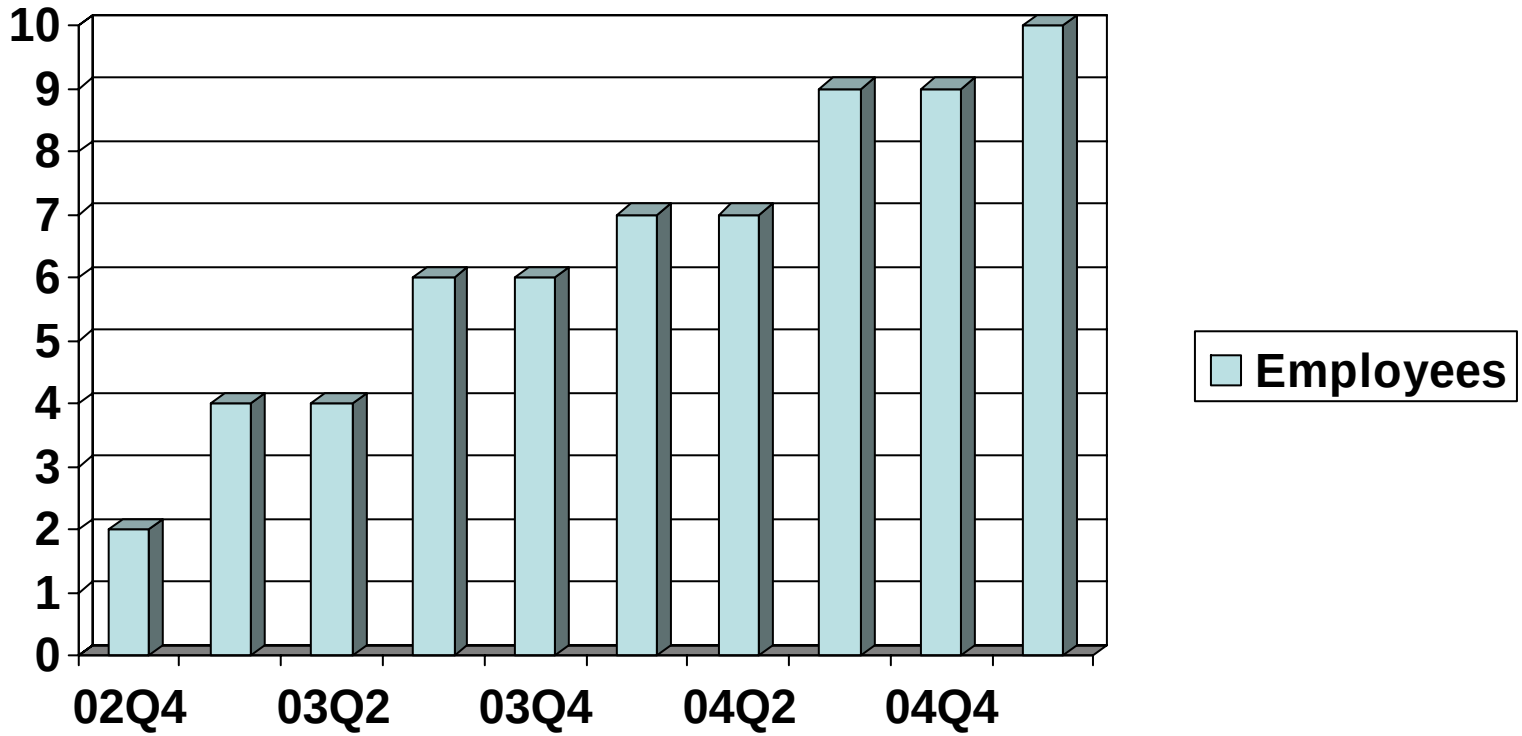
Constituency

According to the assignment:

- Government authorities
- Municipalities
- Regions
- Companies

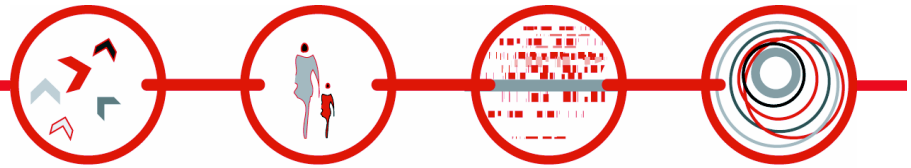


Staff



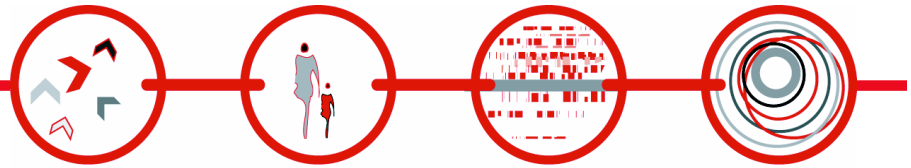
Status Dec 2004

- All four parts of the assignment operational
- 250 Security Advisories
- 30 Security Alerts
- Series of preventive advisories underway
- Quarterly statistical reports
- 9 / 10 employees

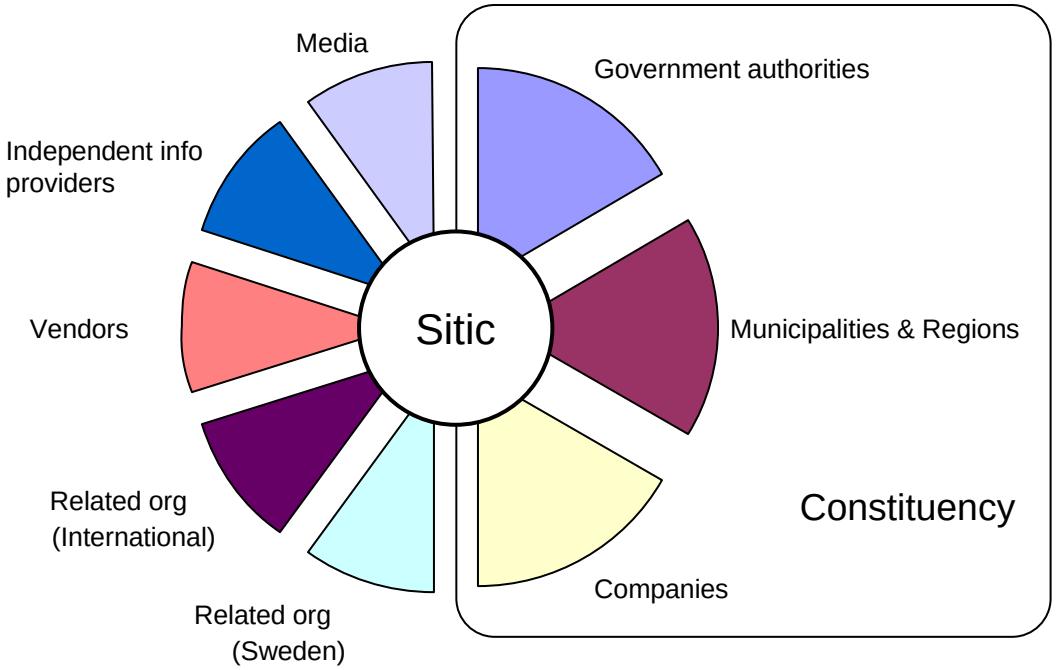


Examples of cases / achievements

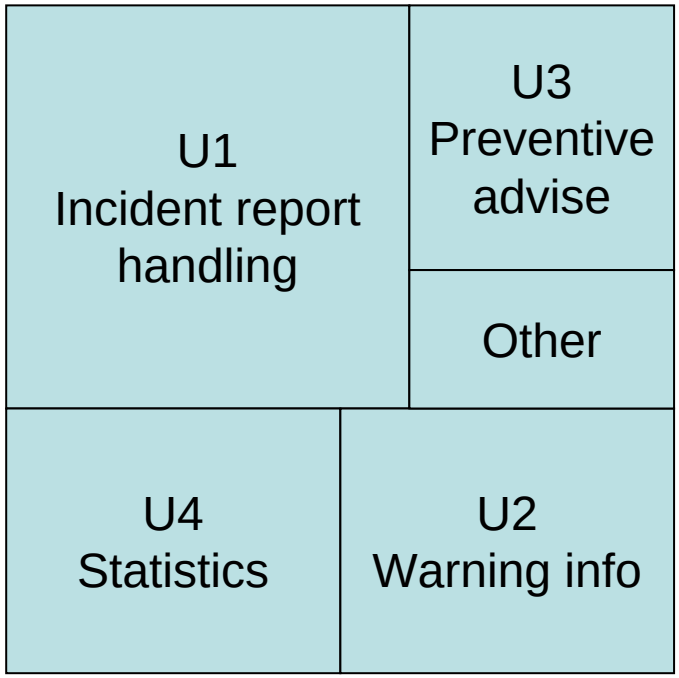
- Co-ordinated international release of vulnerability information
- Implemented (responsible) Vulnerability Disclosure Process for in house discovered vulnerability
- Co-ordination of site closures in phishing case against a Swedish bank
- Incident response and log analysis in DDoS case against a Swedish government agency.
- Security tool development on direct government assignment
- Mass defacement case involving government agencies
- Assistance to municipality in establishing an incident process



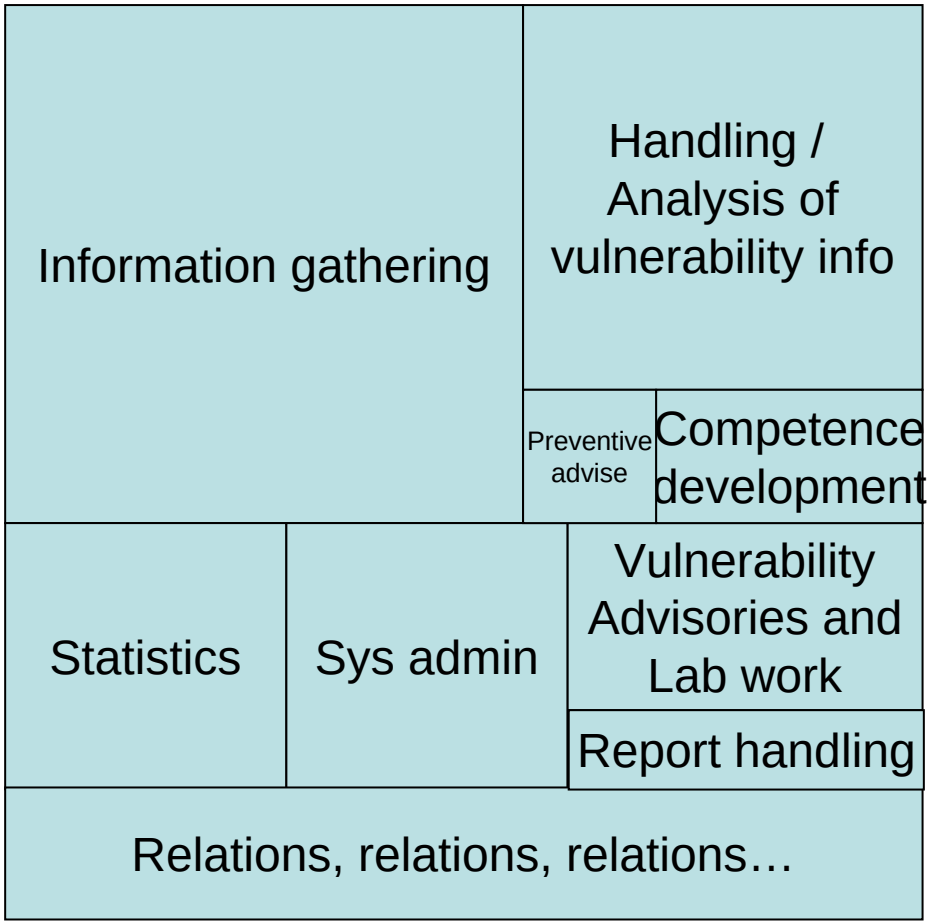
SITIC interfaces



What people think we do

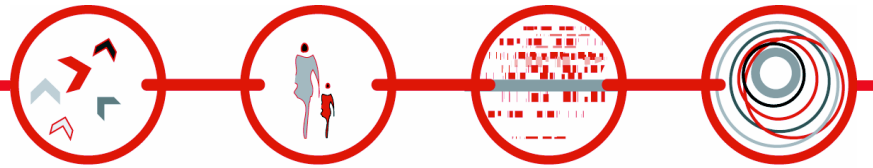


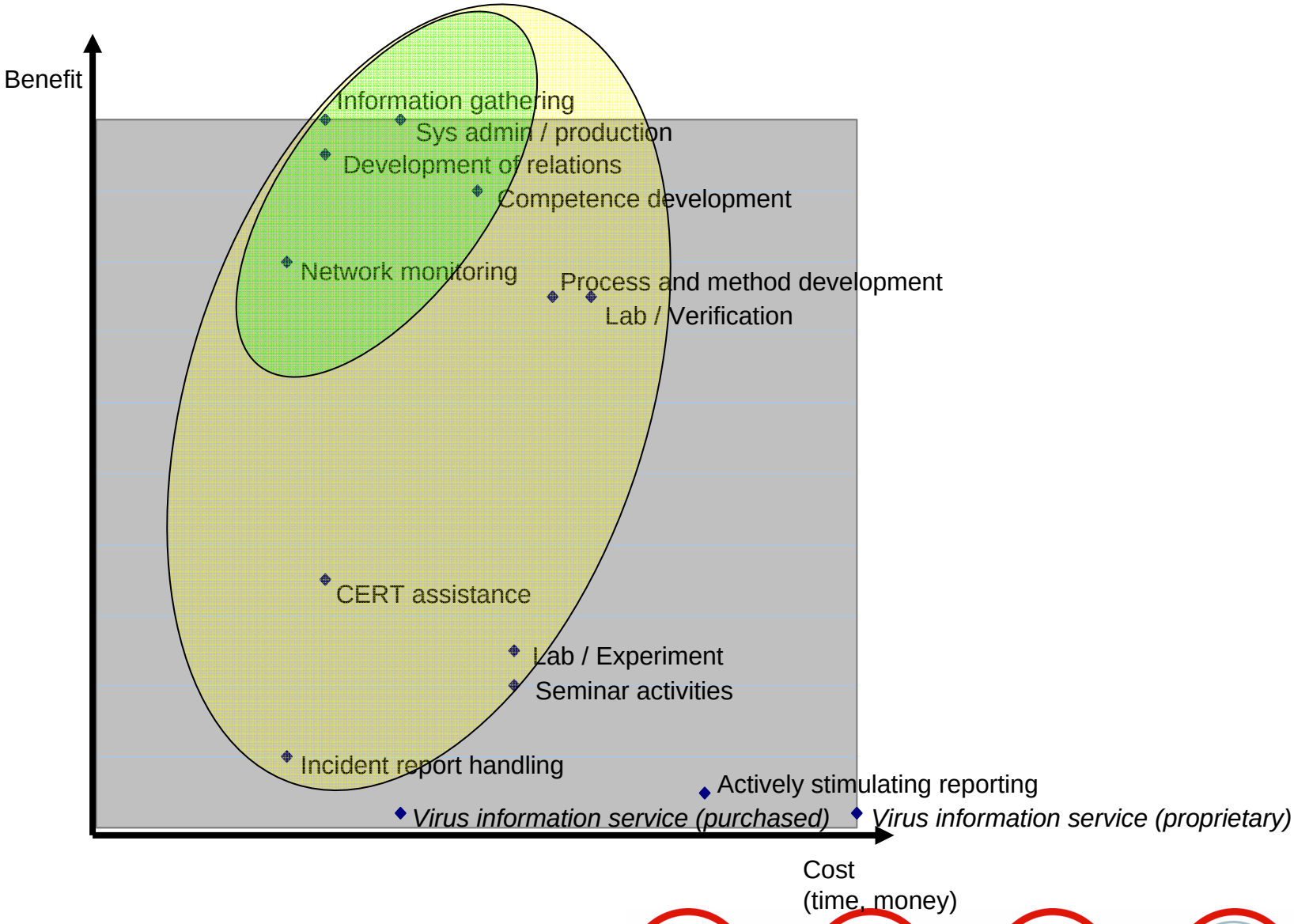
What we actually spend time on



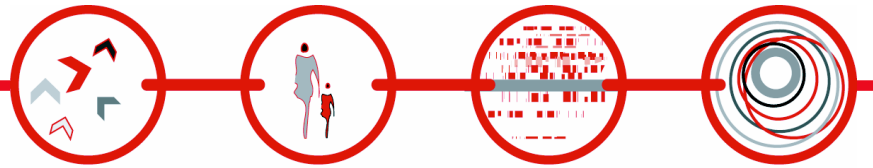
Usefulness of different activities

- Information gathering is key
- Relations are key
- A lab environment is ”a safety net”
- Incident reports have negligible effect on the ability to discover and warn about new threats
- Not owning a substantial production network is limiting
- Network monitoring possibilities provide original, proprietary data, which is key



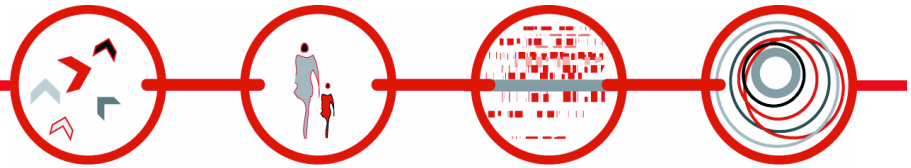

Benefit
Information gathering
Sys admin / production
Development of relations
Competence development
Network monitoring
Process and method development
Lab / Verification
CERT assistance
Lab / Experiment
Seminar activities
Incident report handling
Actively stimulating reporting
Virus information service (purchased)
Virus information service (proprietary)
Cost
(time, money)

Lessons learnt: Handling of incident reports

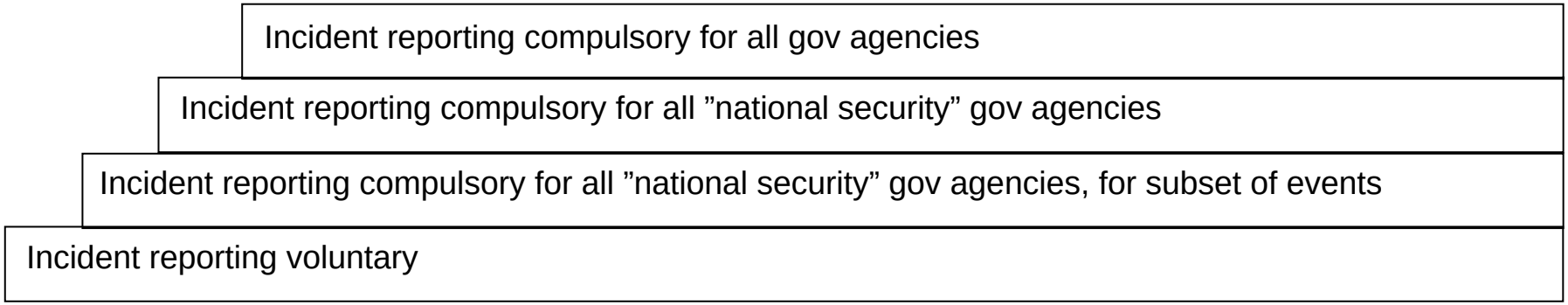


Incident reporting

- (Probably) Lower numbers of incidents in the constituency than originally expected
- Lower willingness to report than expected
- Lower importance for SITIC's other tasks than expected
- Incentive to report is key
- Receiving incident reports primarily for statistical purposes does not motivate 24/7/365 activities

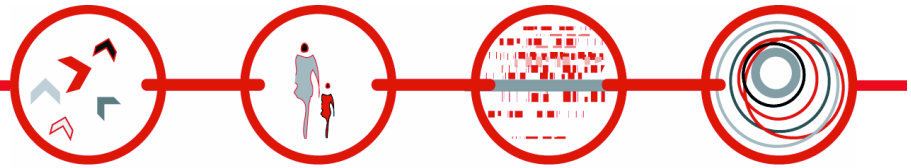


Control levels to consider

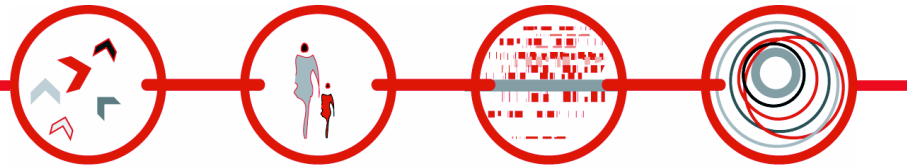


Lessons learnt: Communication regarding threats and risks

- Clear move from incident related work towards work with vulnerabilities and ”help to help yourself”
- Work flow: Documented process and tailored tools are key
- *Develop more SITIC unique info*
- *Investigate non internet dependent info mechanisms (Teletext etc)*
- *Build closer relations with certain vendors (advance info, technical reference)*

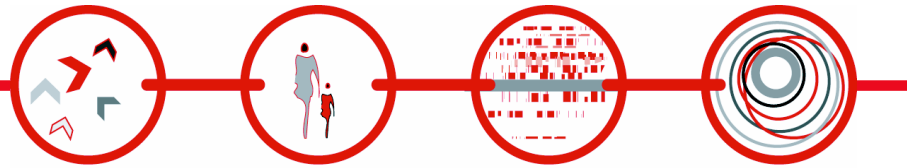


Lessons learnt: Preventive activities

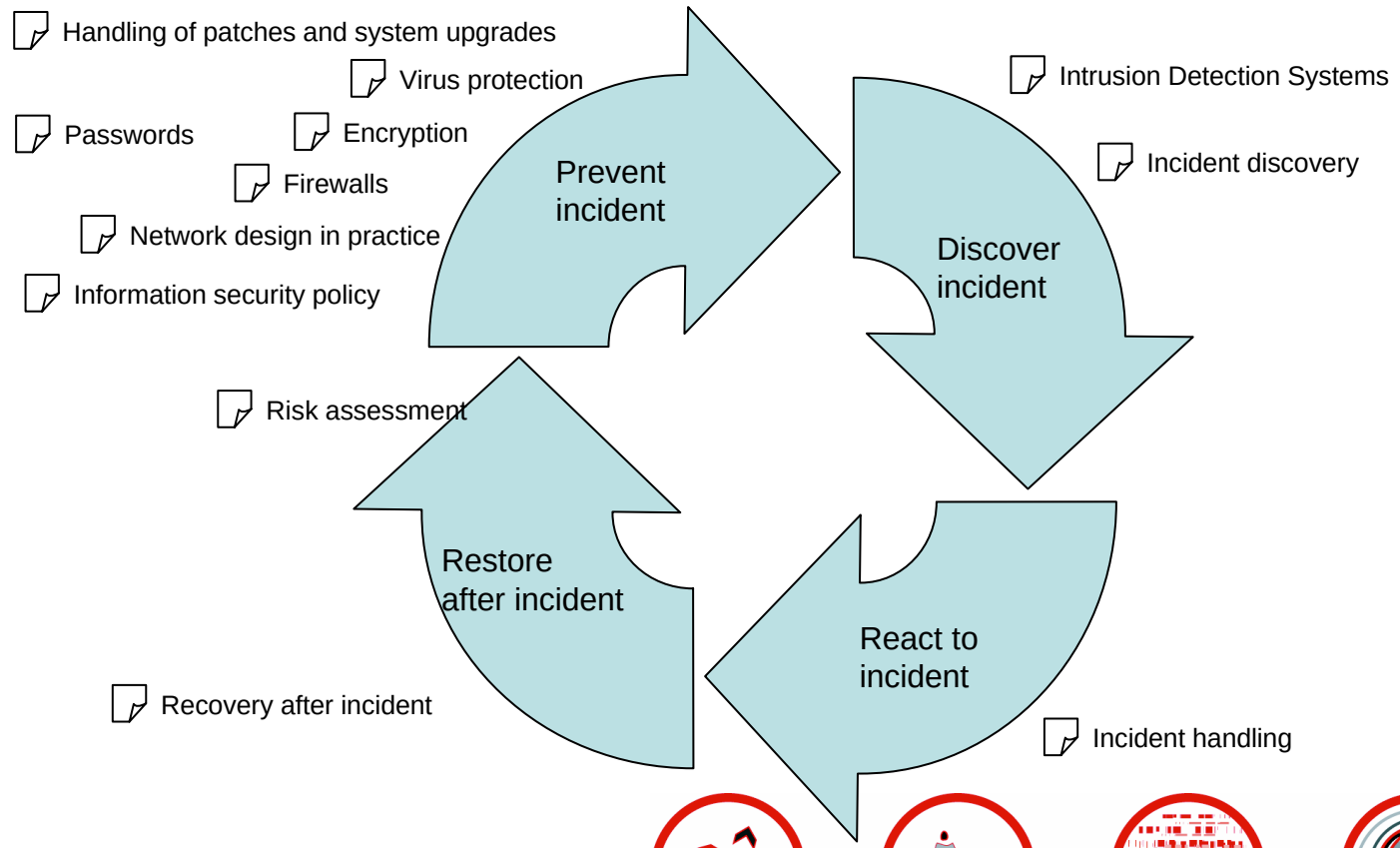


Preventive info, ”best practices”

- Preventive advisories have considerably lower impact than (time critical) advisories and alerts
- Indications are that preventive advisories become interesting only when a security problem has occured
- What type of preventive info it is relevant for a CSIRT to provide is unclear (int. comparison)
- Arranging seminars has a low impact / effort ratio

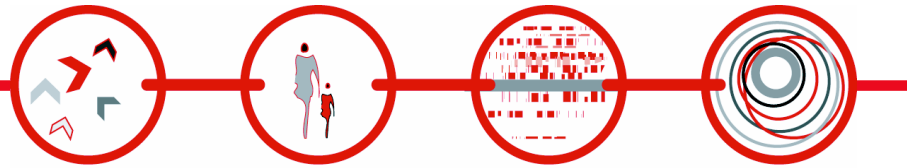


Preventive advisories – SITIC delimitation



Lessons learnt: Statistics

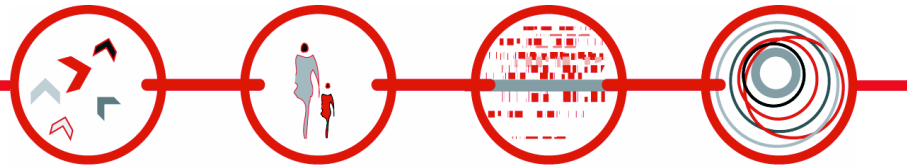
- External statistics are difficult to compare
- Control over data quality requires proprietary info
- Proprietary data is essential for a CSIRT, not having a substantial production network is limiting
- *Build statistics on raw data (logs) from partners*
- *Establish and develop our Distributed IDS*
- *Identify additional external sources for statistics*



International comparison – seeking an identity

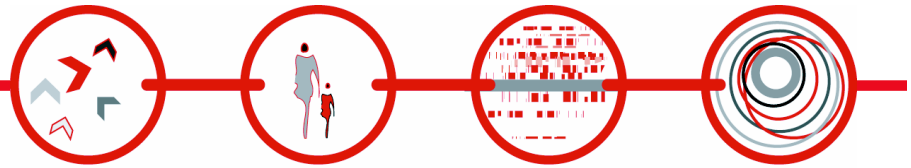
- RFC 2350 “Expectations for Computer Security Incident Response” (chapter 3.5)
- GOVCERT.NL CERT-in-a-box
- CERT/CC ”Handbook for Computer Security Incident Response Teams”

The resulting profile illustrates, to ourselves and to others, what we are and what we are not.



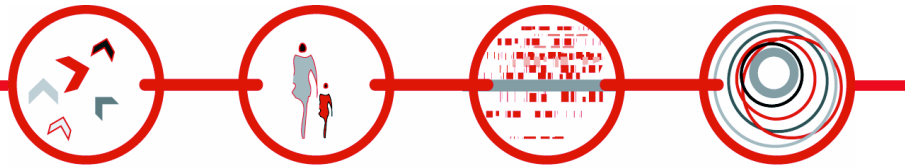
Presentation structure - revisited

- Framework
- Assignment
- Basic facts about the resulting Sitic organisation
- Internal vs External view
- What we learnt
  - General remarks
  - For each task in the assignment
    - *Hints for budding new organisations*



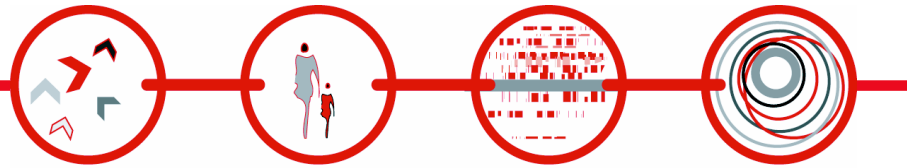
Hints – some key issues for establishing a Government CERT (and perhaps other CERTs)

- An unambiguous **task definition**.
  - The issuers of the assignment are typically not CERT experts.
  - Expectations differ between organisations with vested interests.
- A clear and delimited **mandate**.
  - E.g. authority in networks and organisations.
- A clear and delimited **responsibility**.
  - What can the organisation be held accountable for, when and by whom?



Hints – some key issues for establishing a Government CERT (and perhaps other CERTs) (cont.)

- A complete (secrecy) **legislation**
- **Success factors**
  - What will the organisation be measured on?
- The right **competence** and attitude
- **Publicity**
  - Make yourself known
- Join international **organisations**
  - Work consciously on relations
- **Learn from others**



Swedish IT Incident Centre

Swedish IT Incident centre
National Post and Telecom Agency
P. O. Box 5398
SE-102 49 Stockholm
Tel +46-8-678 57 99
Fax +46-8-678 55 05
sitic@pts.se
www.sitic.se