

# *Survey among European CSIRTs*

**Marco Thorbruegge,  
Baiba Kaskina**

TF-CSIRT, 24.09.2009.



## *Outline*

- **Introduction - Marco**
- **About the survey - Baiba**
- **Survey Analysis - Baiba**
- **Conclusions - Baiba**

CERT

CERT

# *About the Survey*



## *About the Survey*

- 54 questions
- Web-based survey
  - Text file available
- Webropol tool used
- Privacy statement
- Individual links for each respondent

## *Respondents*

- 129 teams invited to participate
- 3 teams added later
- 88 responses collected
- 36 countries responded:
  - EU Member States (except Slovakia)
  - EEA Countries (except Lichtenstein)
  - Accession candidate countries - Croatia and Turkey
  - Israel, Azerbaijan, Georgia, Russia, Ukraine

CERT

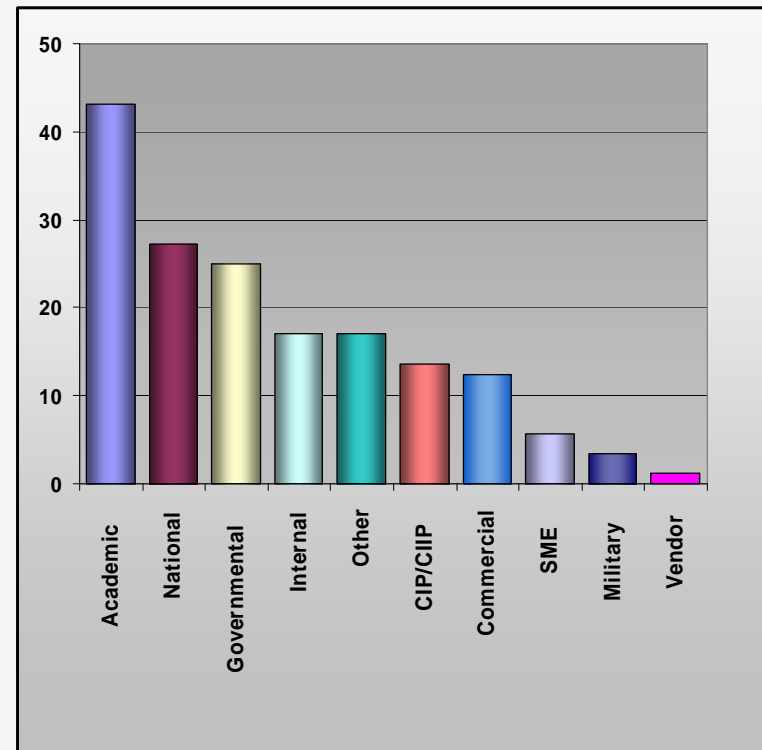
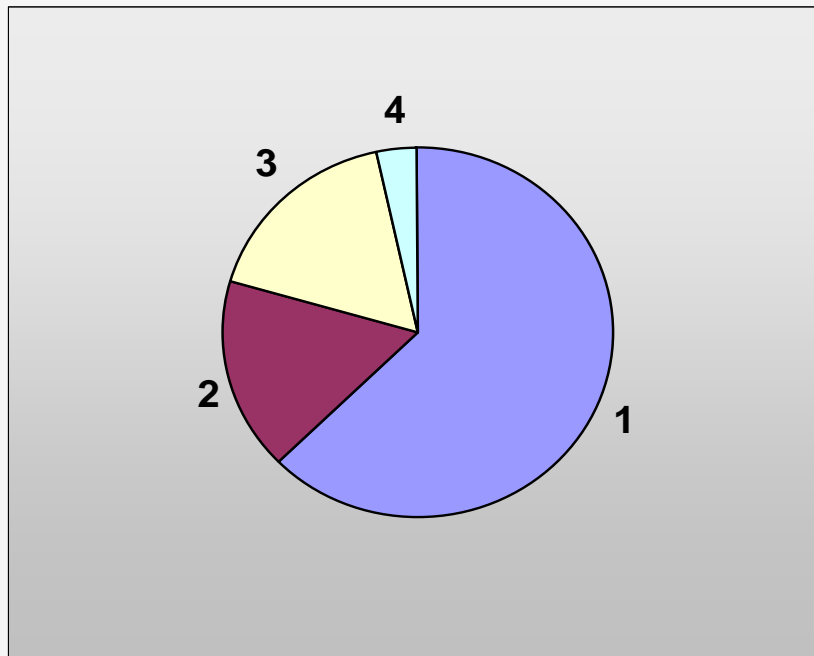
CERT

# *Survey Analysis*

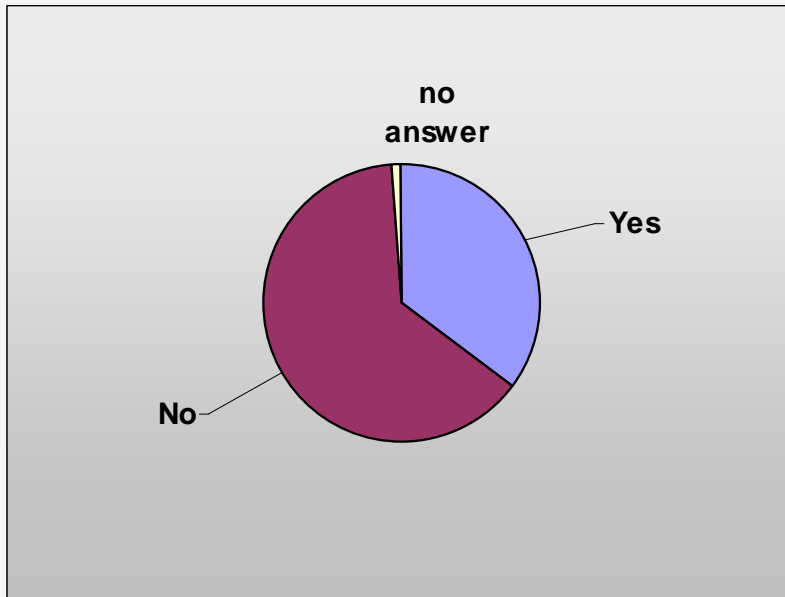


## *CERT constituency*

Number of constituencies for teams:



## ***CERT team acting as (de-facto) national CERT***



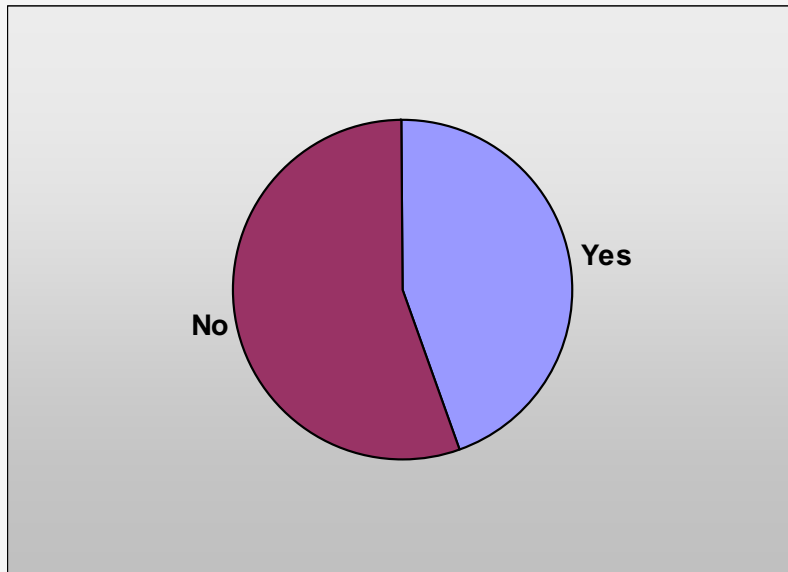
Answers	Number	Percentage
Yes	31	35.2
No	56	63.7
No answer	1	1.1
<b>Total</b>	<b>88</b>	<b>100.0</b>

## ***CERT team acting as (de-facto) governmental CERT***



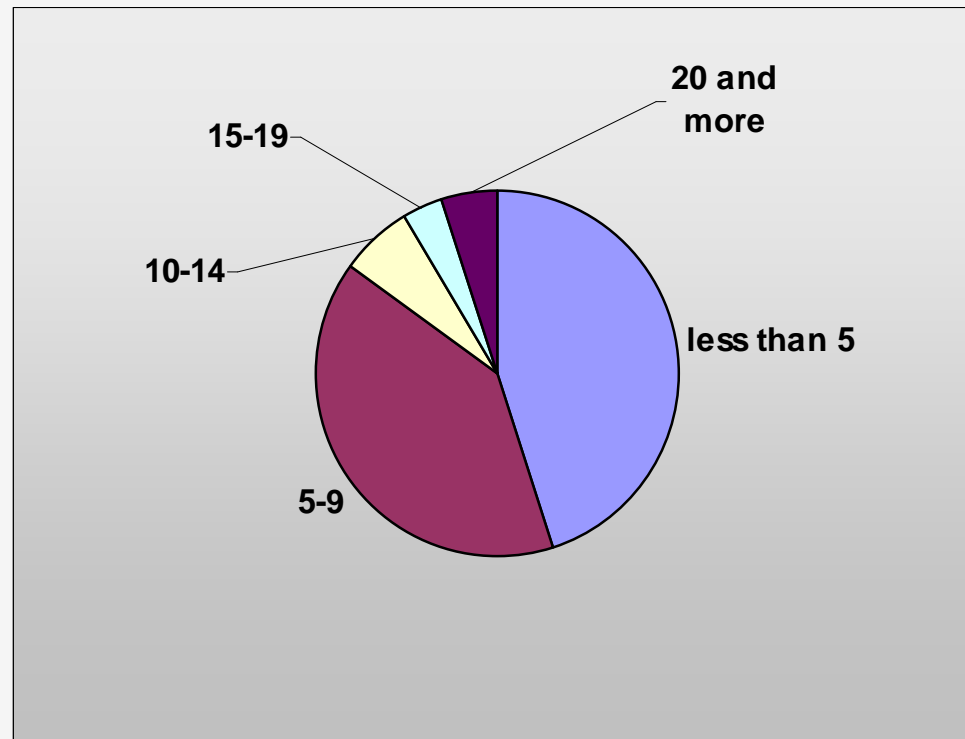
Answers	Number	Percentage
Yes	23	26.1
No	61	69.4
No answer	4	4.5
<b>Total</b>	<b>88</b>	<b>100.0</b>

## ***CERT team acting as national Point of Contact (PoC) or as a "last resort CERT"***



Answers	Number	Percentage
Yes	39	44.3
No	49	55.7
No answer	0	0
<b>Total</b>	<b>88</b>	<b>100.0</b>

## *CERTs by number of team members*



## *Services*

- Reactive Services
- Proactive Services
- Artifacts
- Security Quality Management Services

## ***Security Service Completeness Indexes***

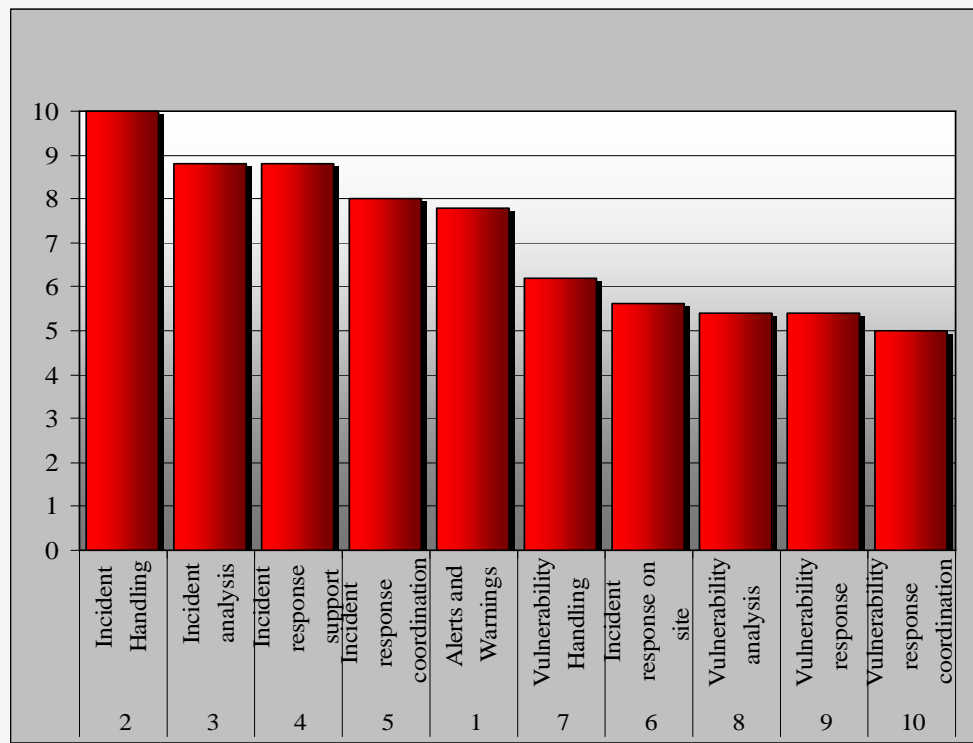
- $S_P$  - the number of provided services
- $S_T$  - the total number of possible services

$$SSCI = \frac{S_P}{S_T}$$

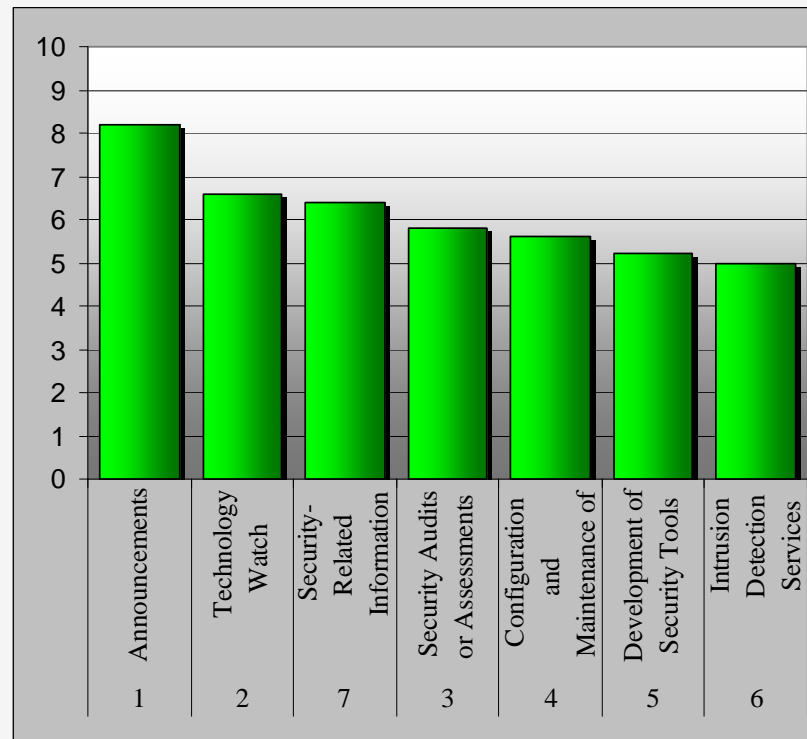
- $W_P$  - the sum of weight coefficients of provided services
- $W_T$  - the sum of weight coefficients of all services

$$SSCI = \frac{W_P}{W_T}$$

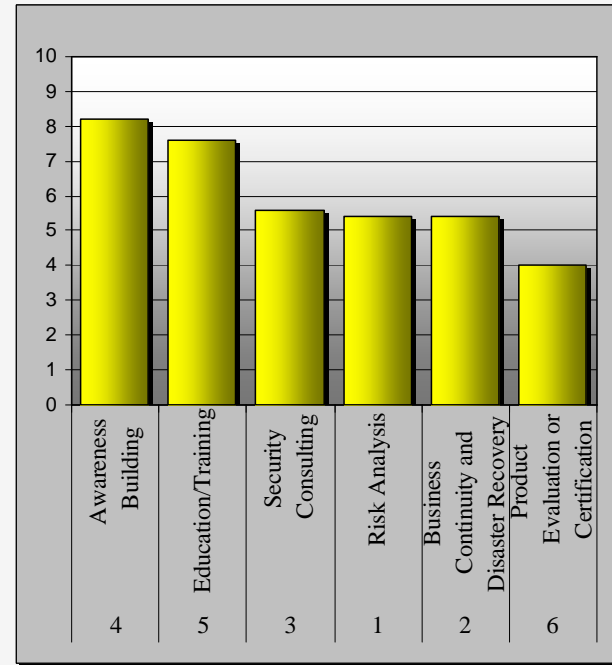
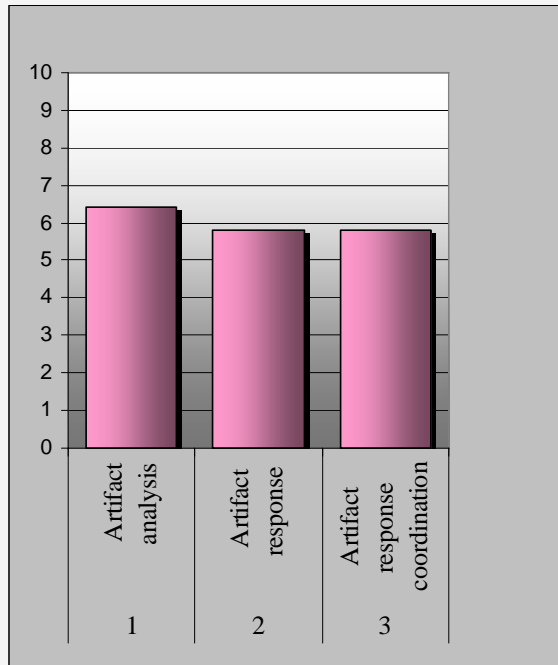
## *The Weight Coefficients – Reactive Services*



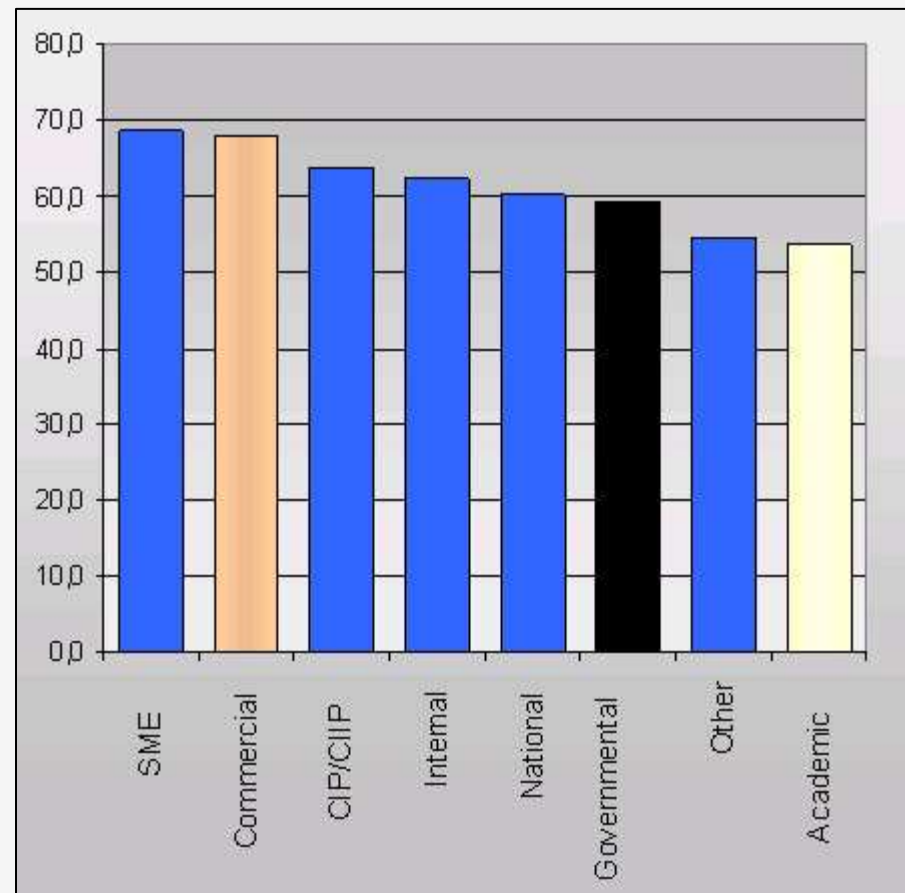
## *The Weight Coefficients – Proactive Services*



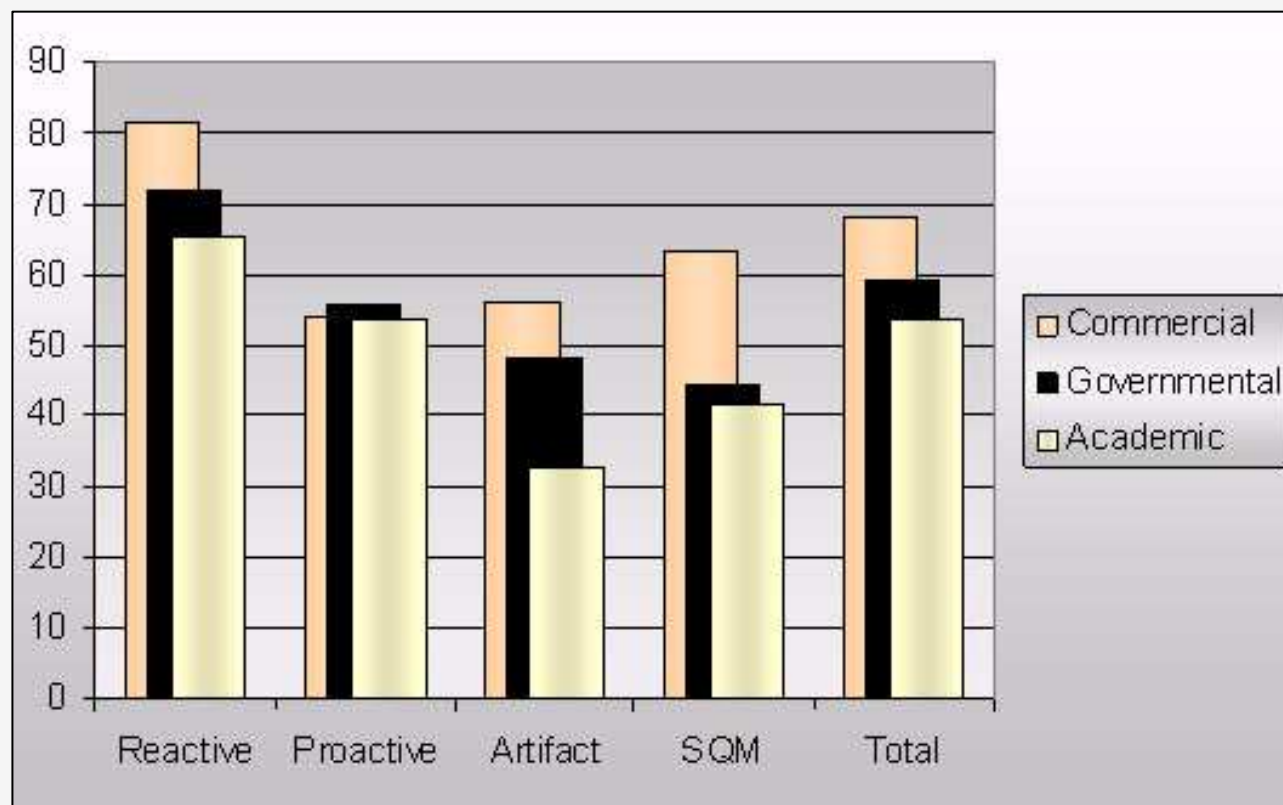
## *The Weight Coefficients – Artifacts and Security Quality Management Services*



## *SSCI for the main constituency sectors*

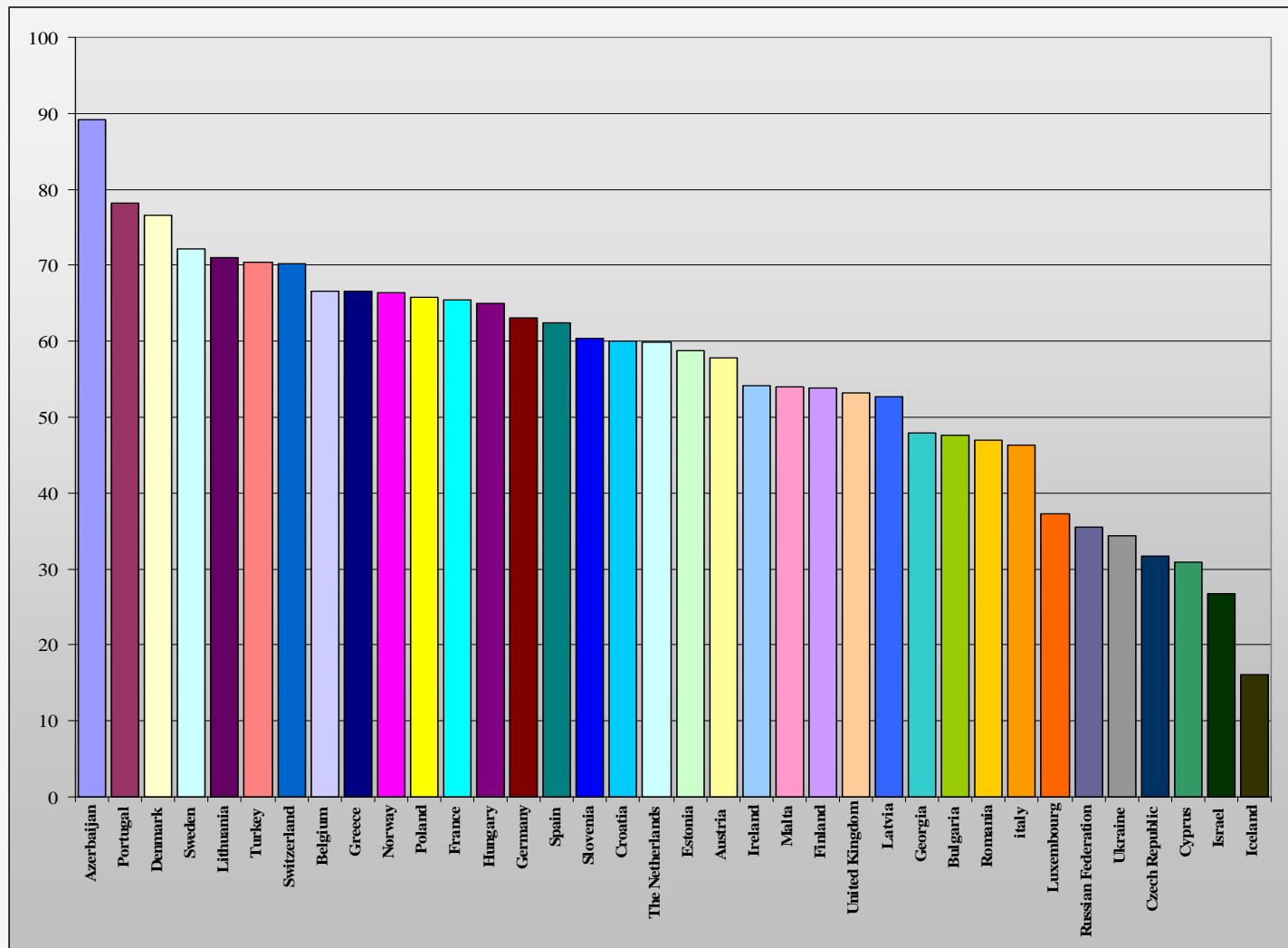


## *Sector comparison graph*

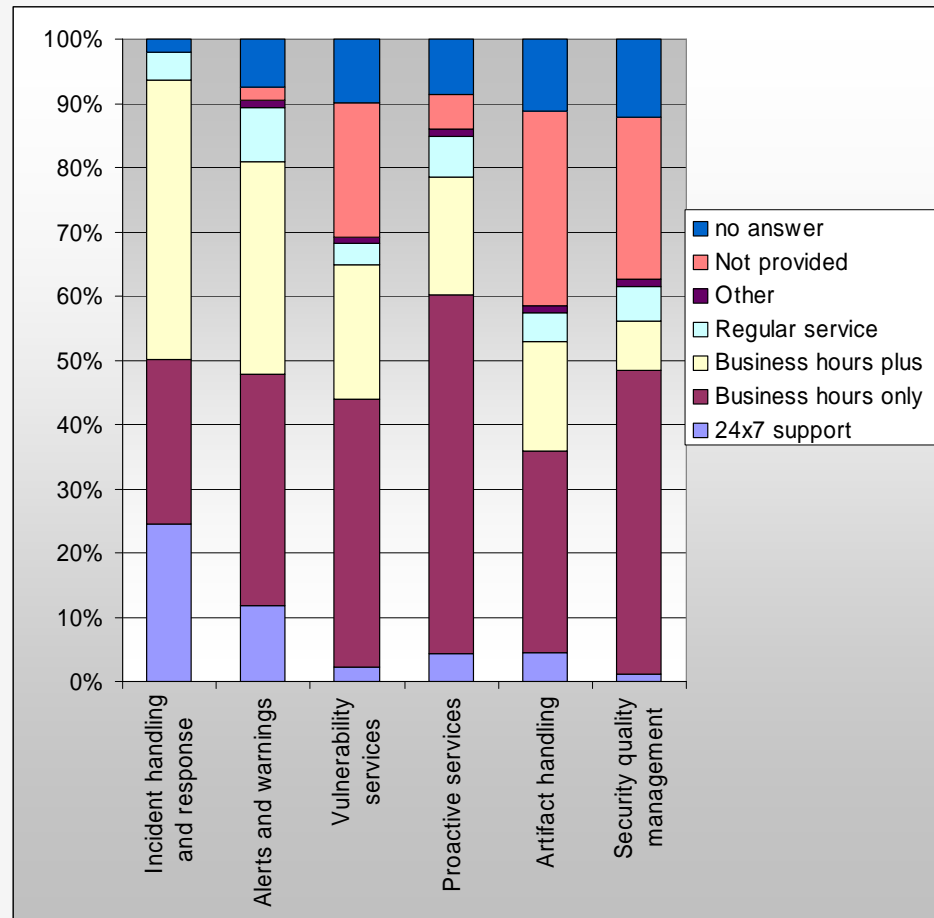




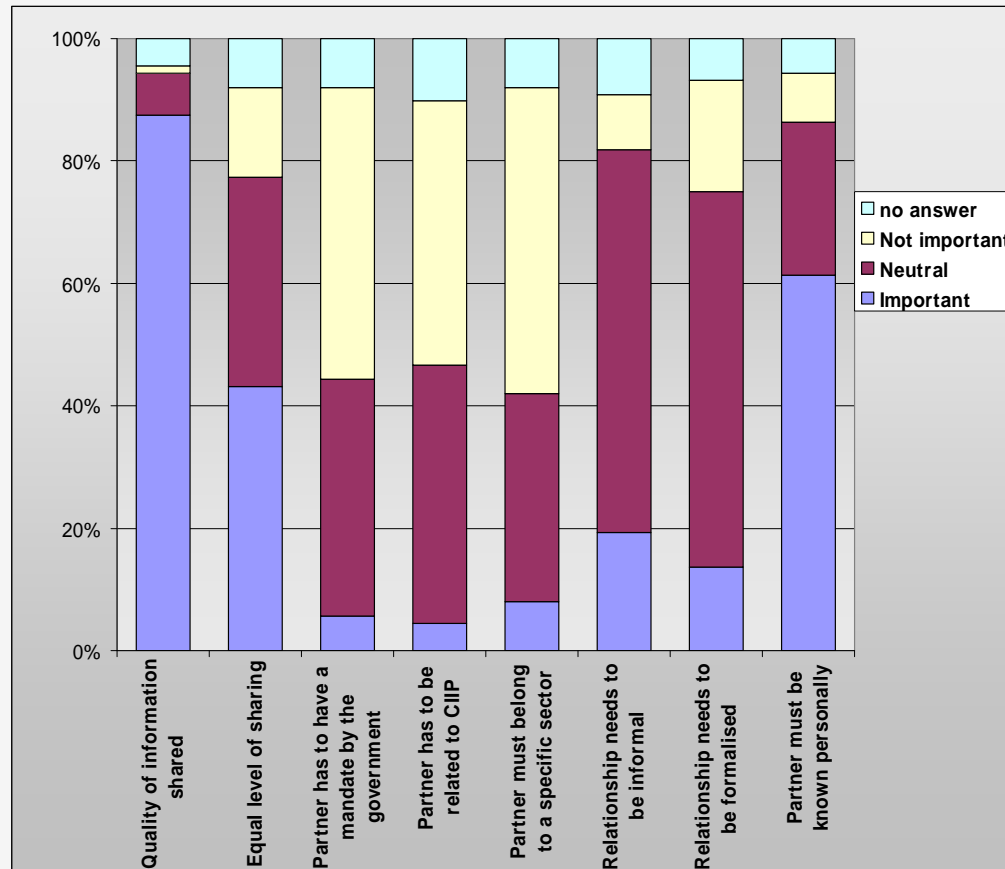
## Average SSCI of the CERTs operating in a country



## Operational modes for services



## Main requirements for successful information sharing



CERT

CERT

# *Conclusions*



## *Conclusions 1*

- Coordination of computer emergency response on the national level is not equally developed in EU countries
- Number of team members is very diverse, but, in most cases, it does not exceed 5 FTEs

## *Conclusions 2*

- Academic sector CERTs provide fewer services than those for the Commercial sector
- Outsourcing is much more popular among the Governmental CERTs than among Academic CERTs

## ***Conclusions 3***

- For all groups of services, the most popular mode is “Business hours only”,
- Only Incident handling and response is provided by most CERTs in the mode “Business hours plus emergency”

## *Conclusions 4*

- Not all teams know about other teams in their country
- The formal international relations of CERTs are undeveloped
- Personal contacts are prevailing legal basis for international relations

## ***Thanks to:***

- *All responded CERT teams*
- *ENISA team*
- *Independent experts*
- *Survey project team*

CERT

CERT

# *Questions?*

*cert-survey@nic.lv*

