

LITNET CERT success story

Marius Urkis

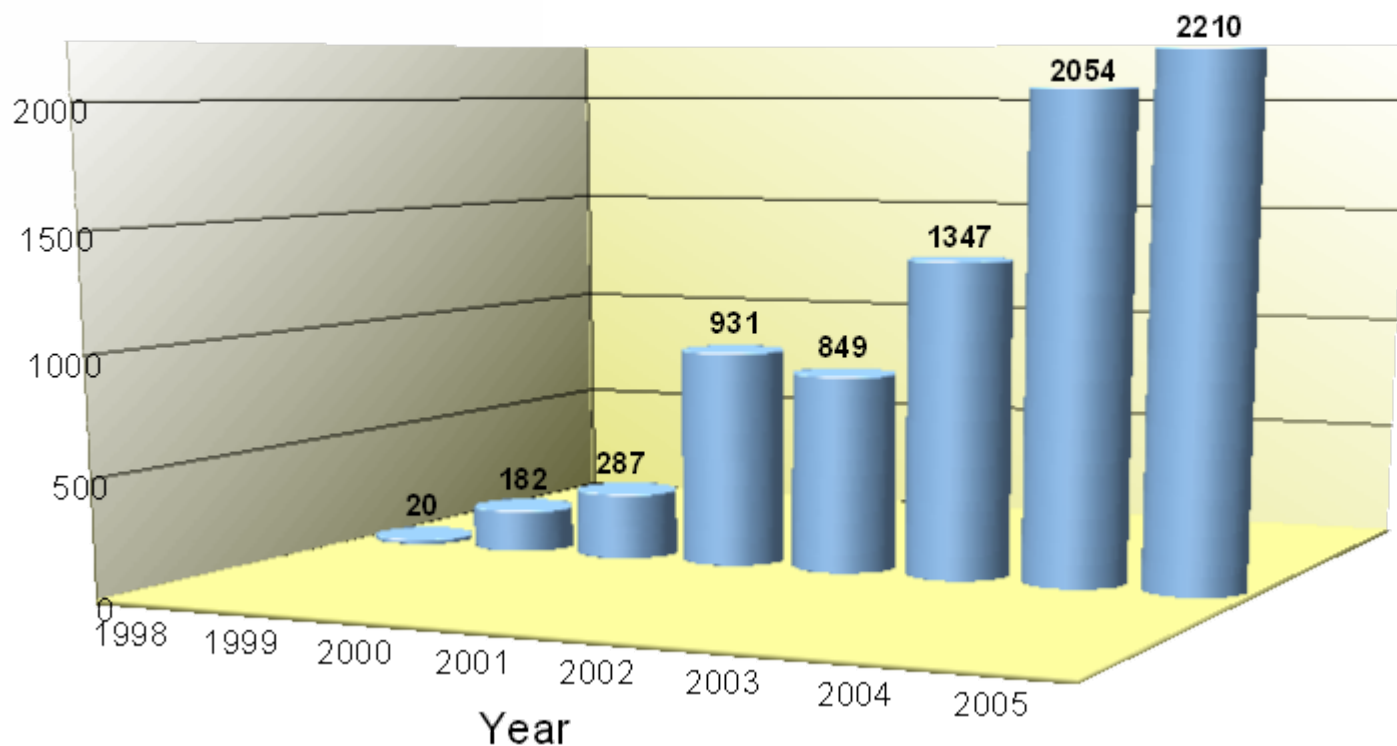
marius@litnet.lt

What is the
SUCCESS
for CSIRT?

Number of incidents declines ?

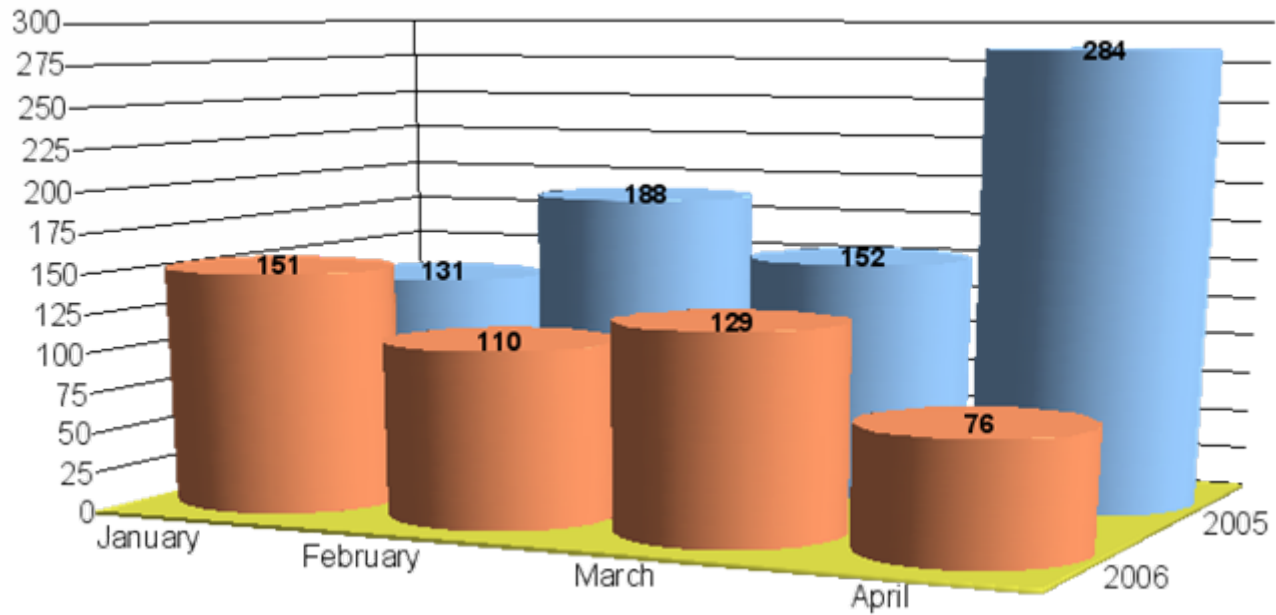
- Evolving technologies = Increasing threats

Security incidents, 1998-2005



Success????

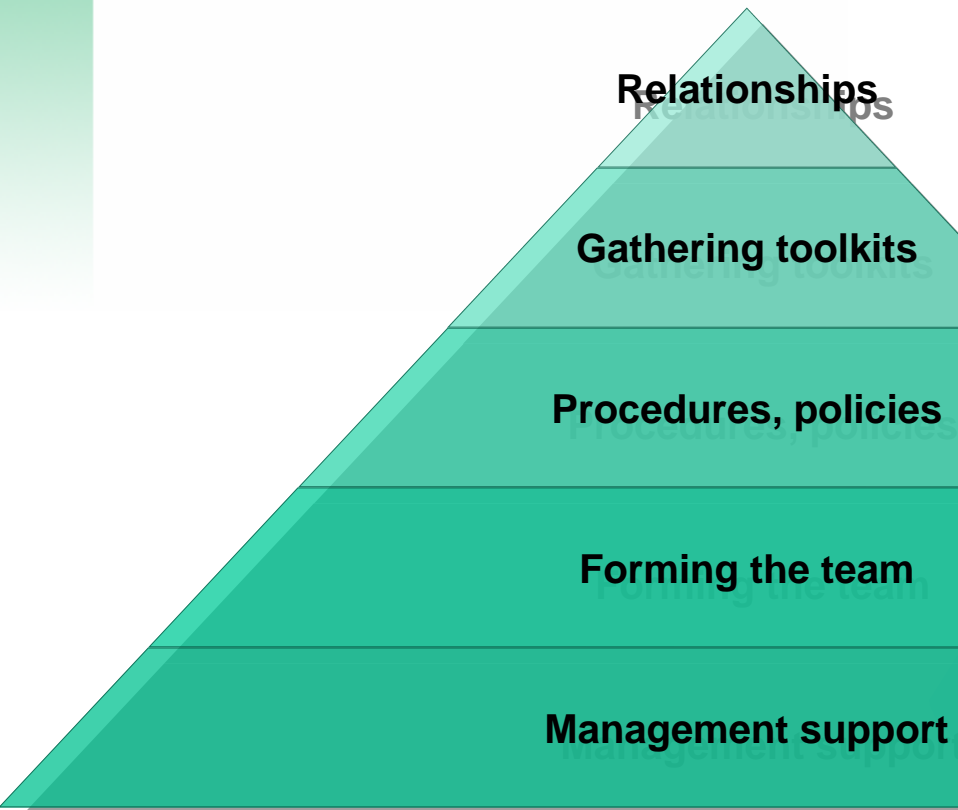
Incidents in 4 months



Number of reports increases

- Increasing trust from constituency ?
- Long term criterion

Our way to success



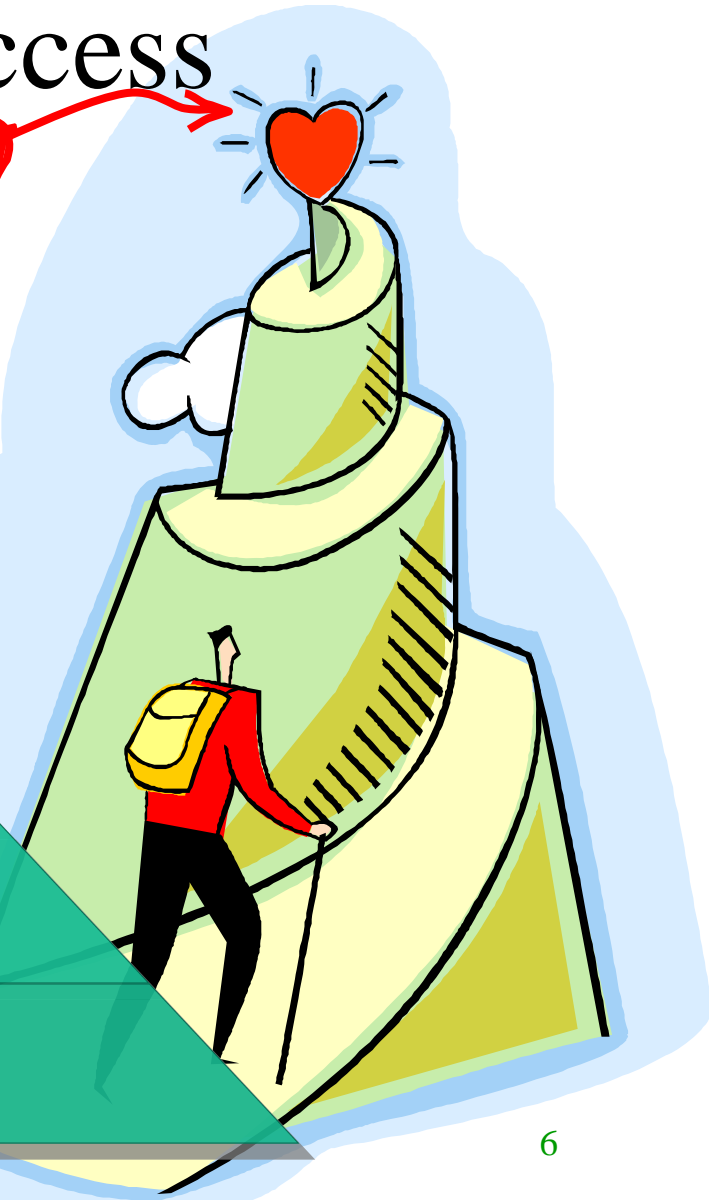
Relationships

Gathering toolkits

Procedures, policies

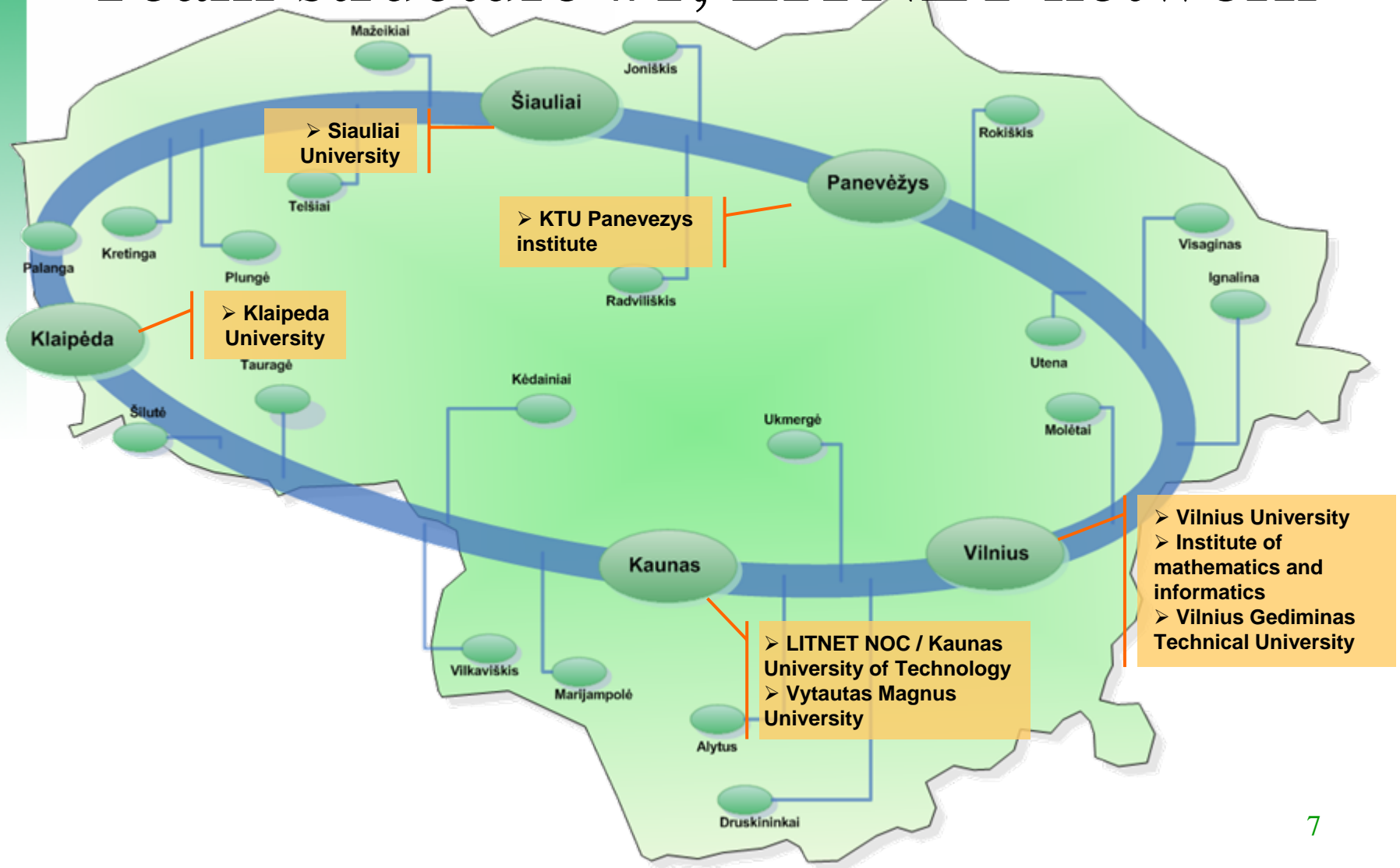
Forming the team

Management support

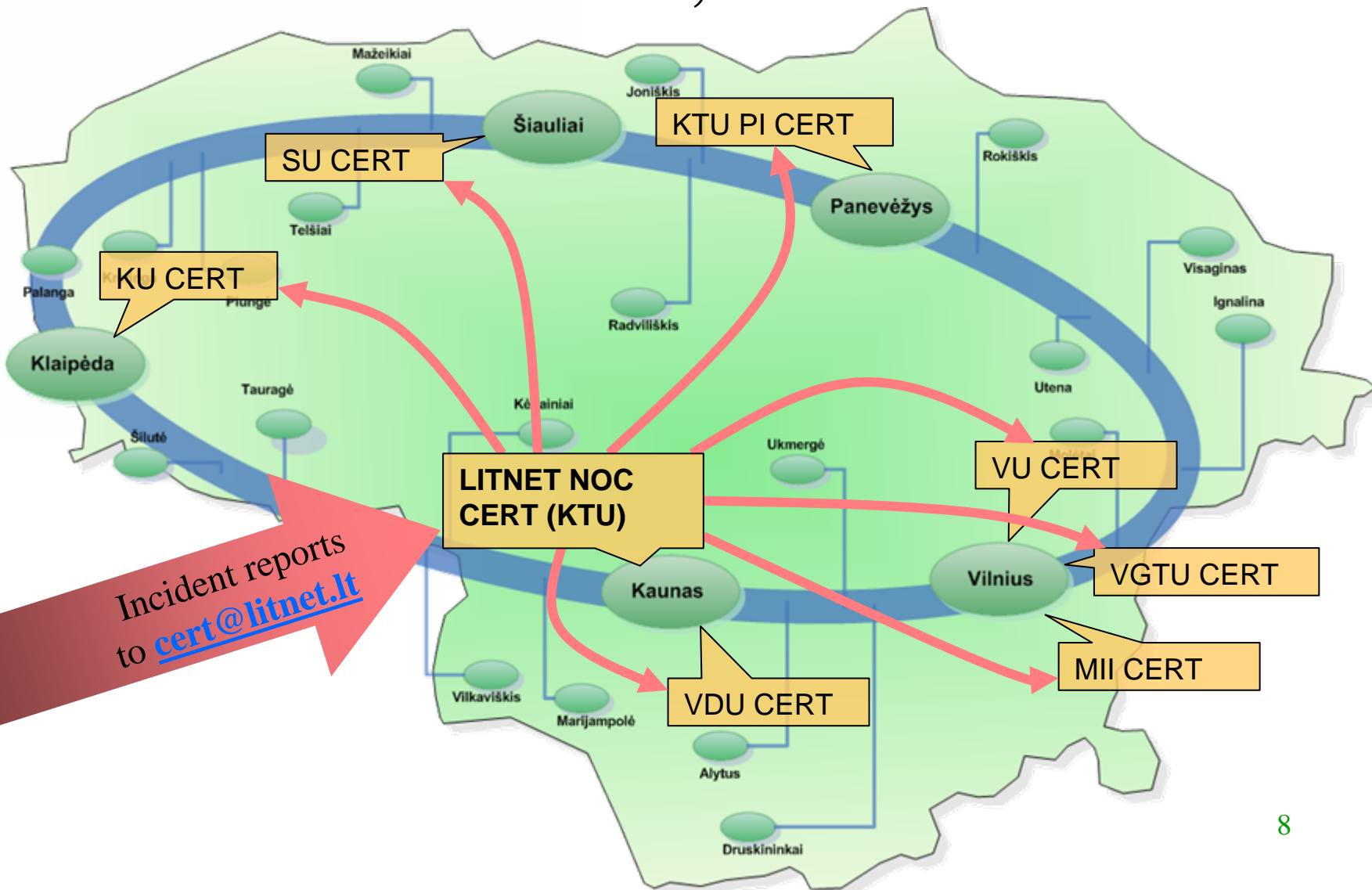


Started in 1998

Team structure #1, LITNET network



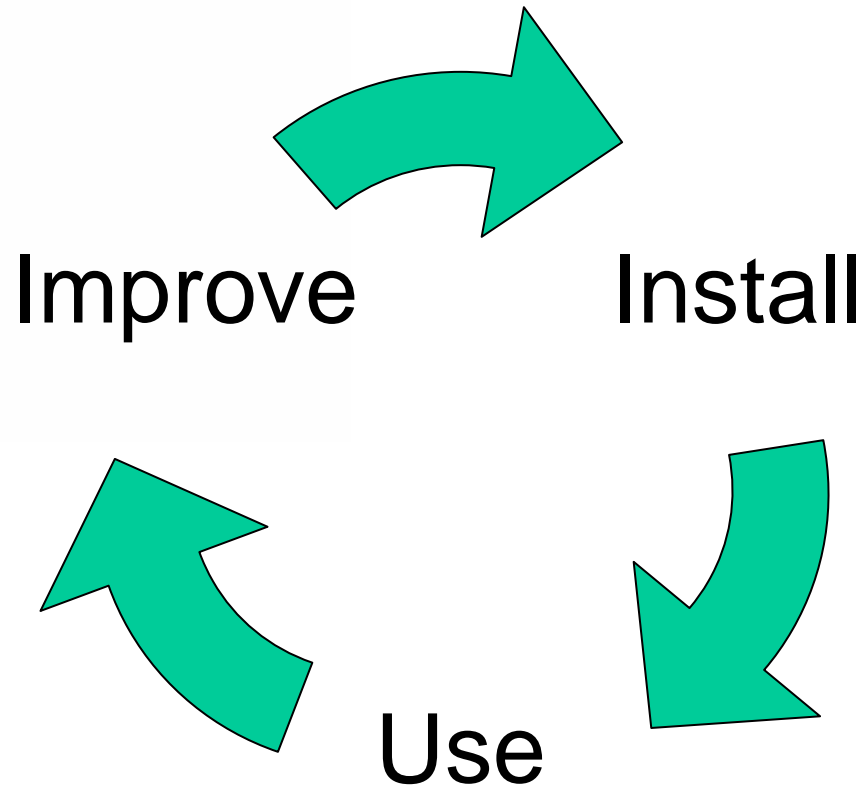
Team structure #2, LITNET CERT



Policies and Procedures

- Policies + Procedures = Quality
 - <http://cert.litnet.lt>
 - RFC2350

Gathering toolkits



Gathering toolkits. Incident management

- Starting with IMAP mbox
- Moved to ticketing system
 - RTIR, <http://bestpractical.com/rtir/>
 - RTIR-WG, <http://www.terena.nl/activities/tf-csirt/rtir.html>

Gathering toolkits. Incident information collection

- Starting with snort + standart snort rules
- Moved to
 - Snort + developed/collected/tested ruleset
 - Netflows/nfsen
 - Input from security community

Relationships with others

➤ TF-CSIRT

- Listed from 2000
- Accredited since 2005

➤ FIRST

- Started with attending annual conf. since 2002
- Member since 2003

Relations with locals

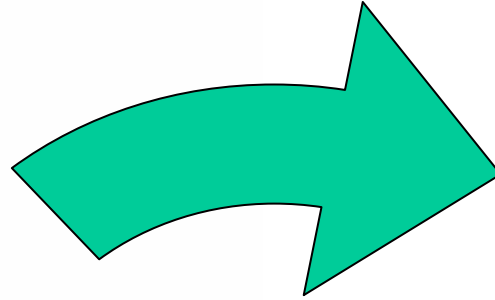
➤ Abuse-LT forum

- Open for lithuanian ISPs, abuse teams, security staff, related organizations
- Place for discussions in security incident/abuse area

User support

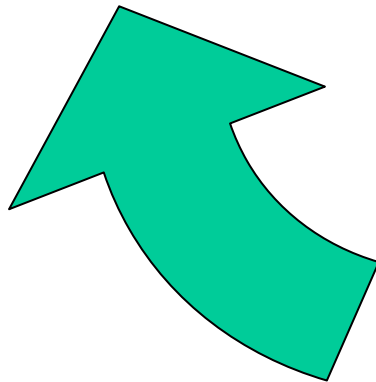
- Education, awareness raising
 - Seminars
 - Security documentation
 - Advisories
- Events, confs.
- Web <http://cert.litnet.lt>
- Mailing lists

And finally...

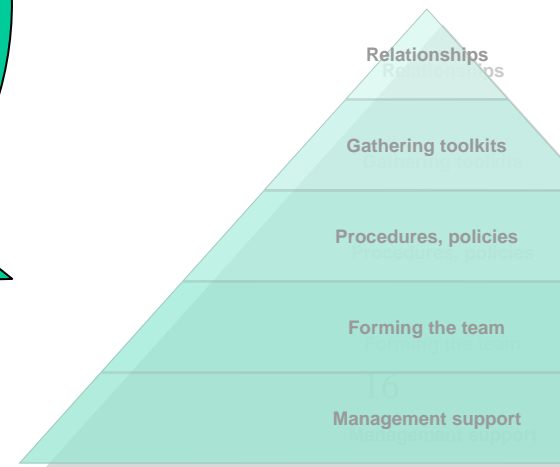
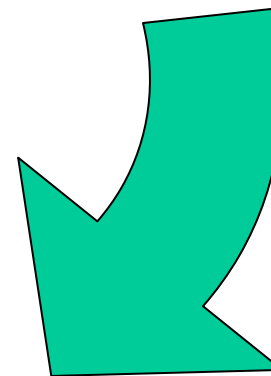


...and improve

Improve



Improve



Relationships

Gathering toolkits

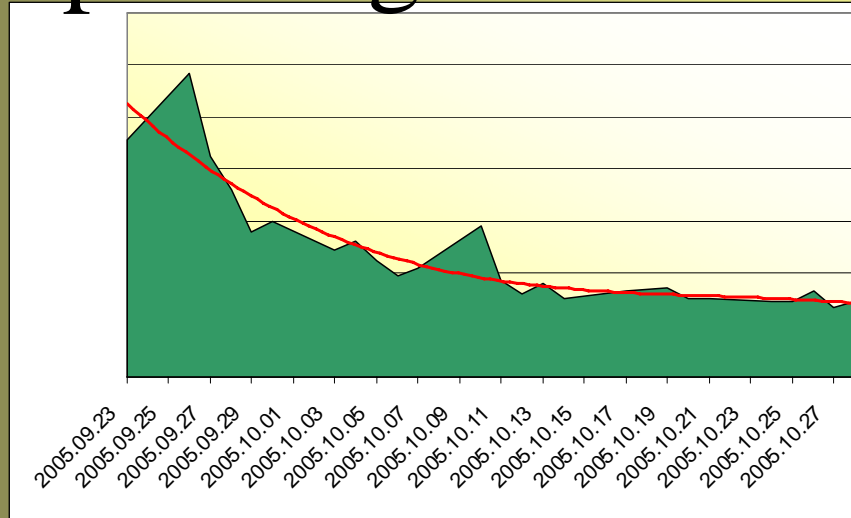
Procedures, policies

Forming the team

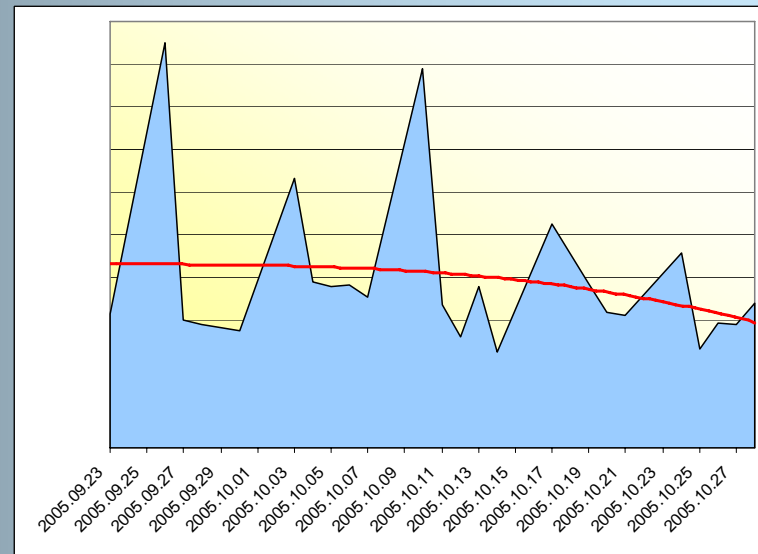
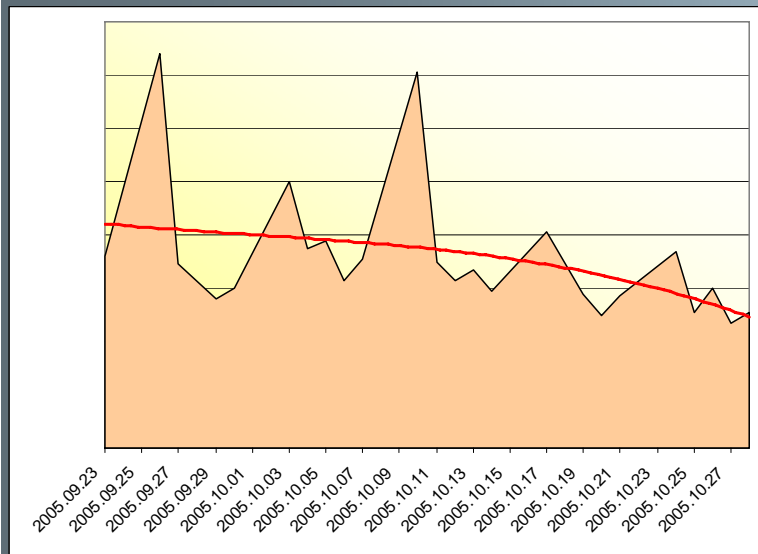
Management support

Is it worth it?

Example: Bagle infection wave

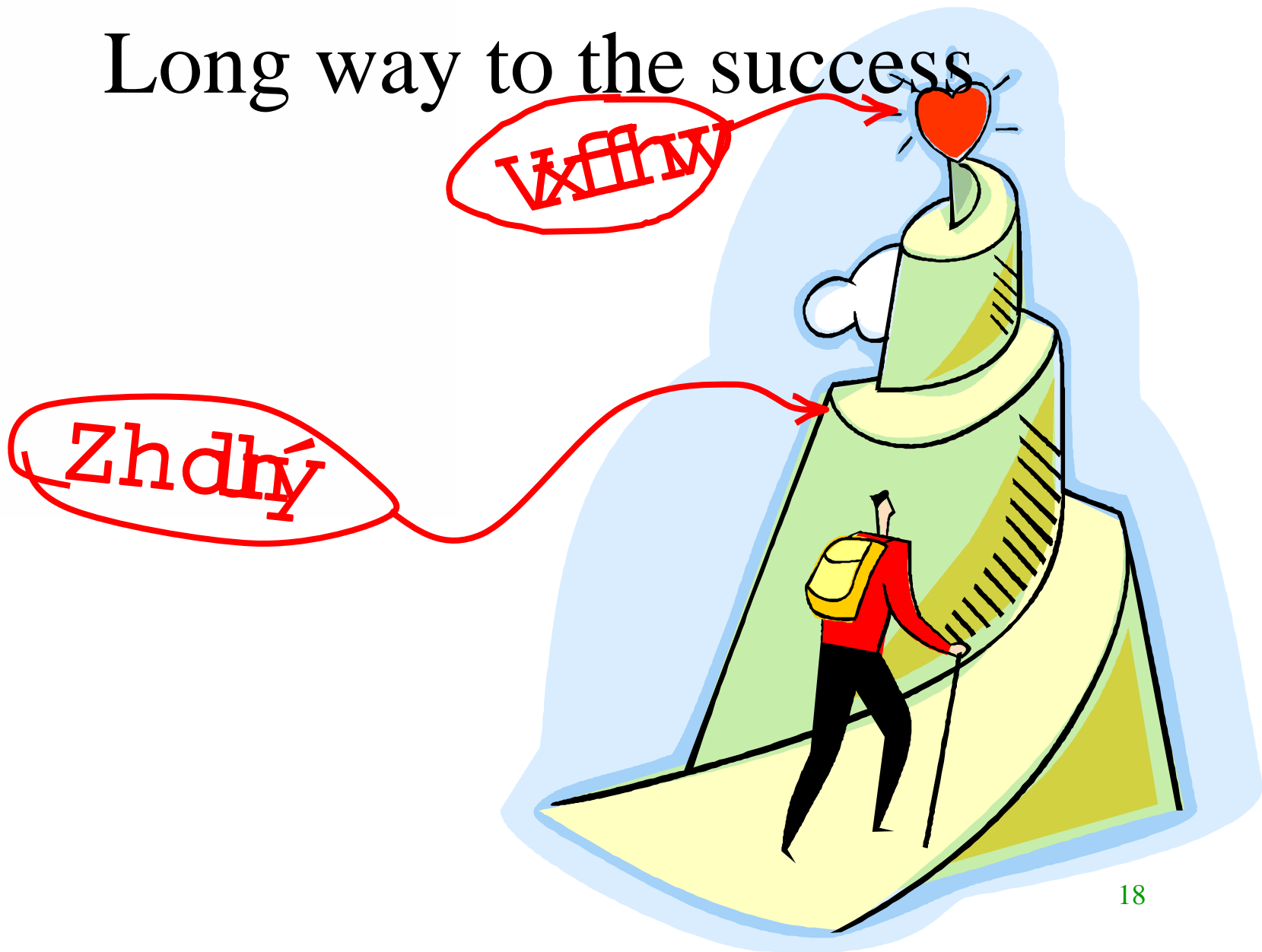


LITNET network



Networks without
CSIRT

Long way to the success



Thank you!

Questions?

