TF-CSIRT
Trusted Introducer

Supporting IT Security Response Teams

2nd ENISA Conference
24 September 2013, Athen, Greece

Dr. Klaus-Peter Kossakowski
kpk@pre-secure.de

Agenda

1. Why was TI established?
2. What is TI?
3. Who is inside the TI community?
4. What kind of Infrastructure is offered?

TF-CSIRT
Trusted Introducer

Why does TI exist?

2nd ENISA Conference
24 September 2013, Athen, Greece

Dr. Klaus-Peter Kossakowski
kpk@pre-secure.de

A Web of Trust takes Work!

- **It started 25 years ago**
  - 1988 CERT/CC established due to crisis
  - 1993 community established in Europe
  - 1998 RFC 2350 published by IETF

A Web of Trust takes Work!

- **It started 25 years ago**
  - 1988 CERT/CC established due to crisis
  - 1993 community established in Europe
  - 1998 RFC 2350 published by IETF
- **In 2000 a more formal approach was needed**
  - Too many teams in Europe
  - No scalable framework

TF-CSIRT
Trusted Introducer

What is TI actually doing?

2nd ENISA Conference
24 September 2013, Athen, Greece

Dr. Klaus-Peter Kossakowski
kpk@pre-secure.de

TI Framework

- **Maintain a community-driven approach for collecting information about response teams**
- **Act as “introducer” for response teams that want to become part of the community**
- **Provide infrastructure support for the community**
  - Workgroups for development / research
  - Collaboration for day-to-day work

Different Levels of „Inside“

- **LISTED or REGISTERED teams**
  - Anyone recognized as response team
  - supported by the TI community
- **ACCREDITED teams, must be REGISTERED**
  - Go through an initial accreditation process
  - Have to adhere to fundamental principles
- **CERTIFIED teams, must be ACCREDITED**
  - Go through workshop and assessment
  - Have to proof maturity and ability

TF-CSIRT
Trusted Introducer

TI Principles

- **Transparency**
  - Allow others to understand your team
- **Setting realistic expectations**
  - Don't promise something you cannot do
- **Respect the interests of other teams**
  - But explain your interests to others also
- **Contribute to the community objectives**
  - Help responding to incidents

TF-CSIRT
Trusted Introducer

Who is inside TI?

2nd ENISA Conference
24 September 2013, Athen, Greece

Dr. Klaus-Peter Kossakowski
kpk@pre-secure.de

TF-CSIRT
Trusted Introducer

https://www.trusted-introducer.org/directory/teams.html

The following list contains all "Listed" teams. "Accredited" and "Certified" teams are - by definition - also "listed" teams, and are therefore contained in this list for your convenience.

Search

Clear all filters

Toggle team details

Filter by State

Clear Filter

- Certified (1)
- Accredited (1)
- Listed (2)
- Candidate (0)

Filter by Const. Type

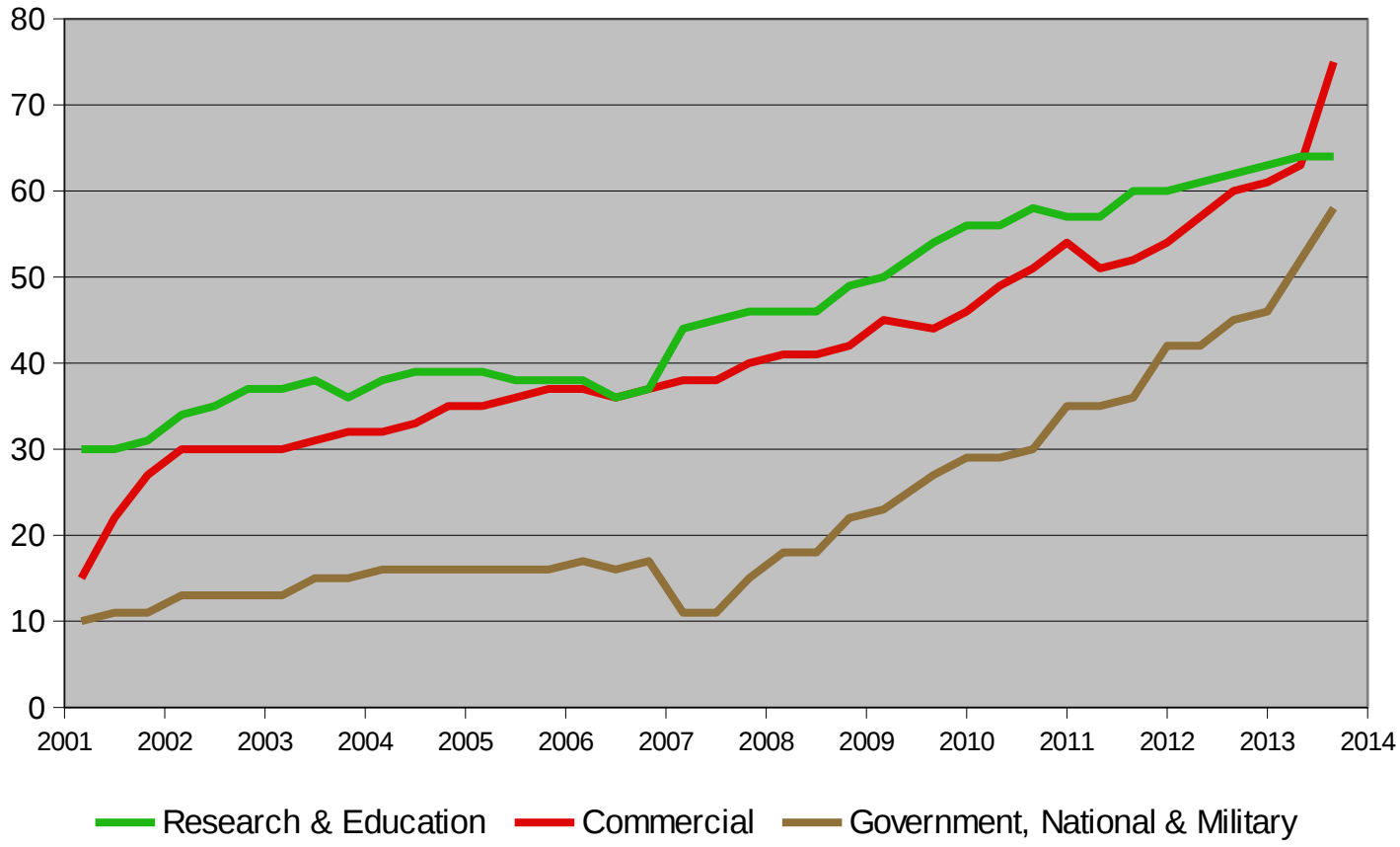
Clear Filter

- Research & Education (2)
- ISP Customer Base (0)
- Vendor Customer Base (0)
- Financial Sector (0)
- Commercial Organisation (0)
- Service Provider Customer Base (1)

Filter by Country

AUTH-CERT Greece	Last updated on 14 Mar 2011	**Listed** since 15 Jun 2004
FORTHcert Greece	Last updated on 12 Jul 2013	**Certified** since 31 Oct 2012
GRNET-CERT Greece	Last updated on 19 Aug 2013	**Accredited** since 07 Apr 2003
NCERT-GR Greece	Never updated	**Listed** since 06 Sep 2011

Listed Teams



TF-CSIRT
Trusted Introducer

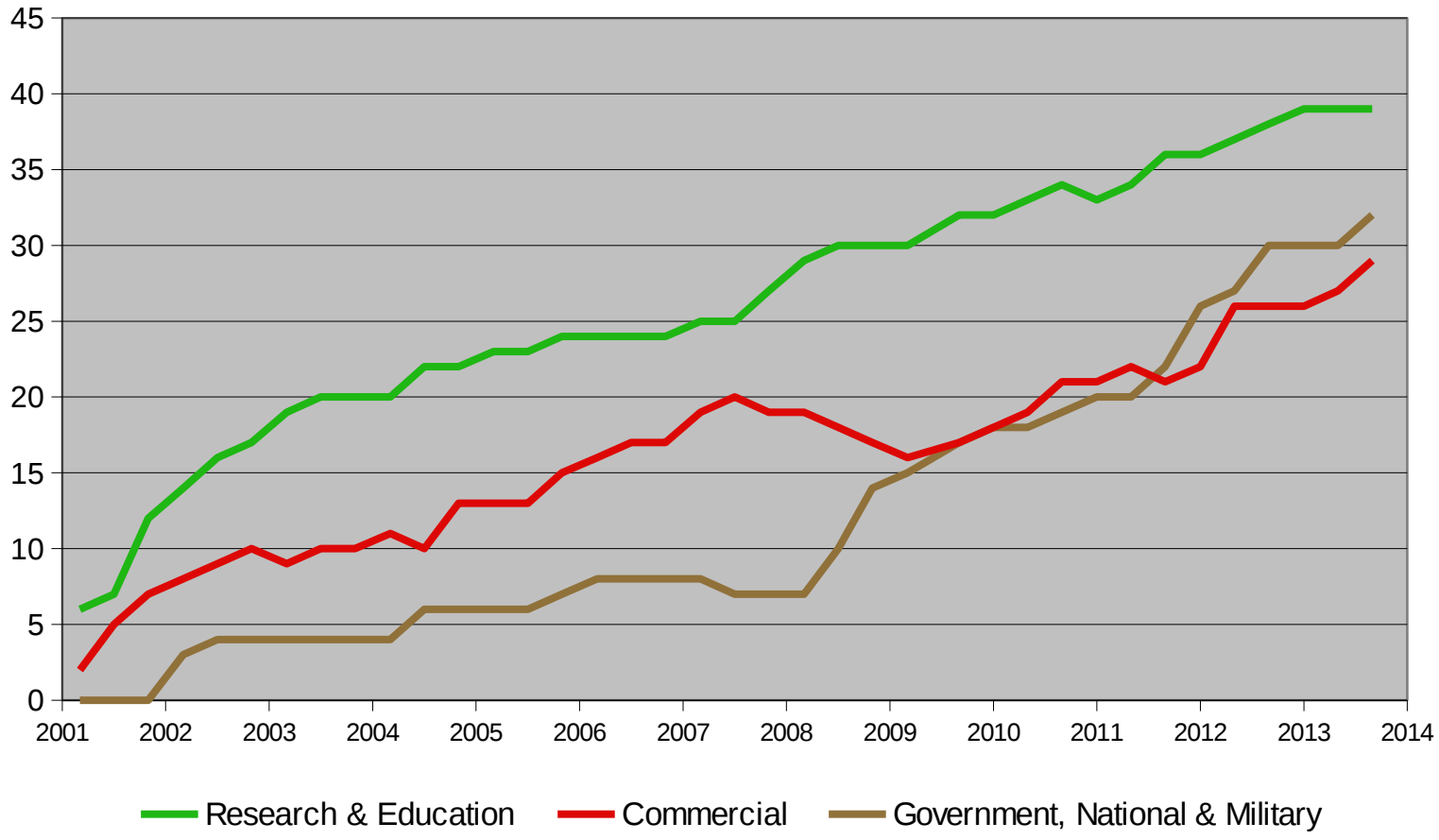
Recent Additions

- aeCERT (United Arab Emirates)
- CERT BWI (Germany)
- CERTGOVIL (Israel)
- DefCERT (The Netherlands)
- LTU MOD CIRT (Lithuania)
- Qatar CERT (Qatar)

Recent Additions (2)

- AAB GCIRT
  (The Netherlands)
- BASF gCERT
  (Germany)
- e-LC CSIRT
  (Spain)
- ISPIRIT
  (United Kingdom)
- KPMG-CSIRT
  (United Kingdom)
- RABOBANK SOC
  (The Netherlands)
- RH-ISIRT
  (United States)
- Secunia Research
  (Denmark)
- Telefonica CSIRT
  (Spain)
- TK-CERT
  (Germany)
- Vodafone-CERT
  (Germany)
- XING
  (Germany)

Accredited Teams



Trusted Introducer

Recent Accreditations

- **Government and Military**
  - CERT-EU (Europe)
  - COSDEF-CERT (Spain)
- **Commercial**
  - Panasonic PSIRT (Worldwide)
  - Malware.lu (Luxembourgh)

Certifications

- **Maturity is the key**
  - Capability Maturity Model based on best practices
- **Functional requirements easily incorporated**
  - Important for National CERTs (ENISA's baseline capabilities)

TF-CSIRT
Trusted Introducer

What can be utilized?

2nd ENISA Conference
24 September 2013, Athen, Greece

Dr. Klaus-Peter Kossakowski
kpk@pre-secure.de

TI Database

- **Accredited teams are required to update their entry at least every four (4) months**
  - Self service interface via the web
- **Database Access via the web**
- **Downloads to import in your DB**
  - PGP keys
  - Contact database
  - IP addresses, network space, ASN

TF-CSIRT
Trusted Introducer

Filter by Const. Type

Clear Filter

- [ ] Research & Education (2)
- [ ] ISP Customer Base (0)
- [ ] Vendor Customer Base (0)
- [ ] Financial Sector (0)
- [ ] Commercial Organisation (0)
- [ ] Service Provider Customer Base (1)

Filter by Country

Clear Filter

- [ ] Spain (12)
- [ ] *European Union (1)
- [ ] Finland (5)
- [ ] France (10)
- [ ] Georgia (2)

FORTHcert

Greece

Last updated on 12 Jul 2013

Certified
since 31 Oct 2012

General Information

Established	Host Organisation	Constituency Types
2007		Service Provider Customer Base

Contact Details

Team Email	Main Phone	Emergency Phone
ABUSE@ICS.FORTH.GR	+302810 391648	+302810 391640
Encrypted Mail Support	**Public URLs**	**Timezone**
PGP	http://www.forth.gr/forthcert/	GMT+02 / GMT+03
Business Hours	**Emergency Procedure Phone**	
09:00 to 17:00 Monday to Friday	use e-mail	

Communication Mechanisms

- **Cryptographic Mailing Lists**
  - Protected by X.509 user certificates
  - For the whole community
  - For sub groups as defined by community
- **Cryptographic IRC Server**
  - Protected by X.509 user certificates

Downloads from HTTPS Server

- Protected by X.509 user certificates

Communication Mechanisms (2)

- **Out-of-Band telephone / SMS alerts**
  - Protected by user / team credentials
  - Users can leave a message
  - SMS will alert other users or team roles
  - System will call out to specified telephone numbers and mobile phones

Crisis Management?!?

- **Ad hoc team will be set up by volunteers to**
  - Identify a coordinated approach
  - Utilize TI functions and secretariat support
- **We have the mandate to do good things! However no authority!**

TF-CSIRT
Trusted Introducer

Wrap Up

2nd ENISA Conference
24 September 2013, Athen, Greece

Dr. Klaus-Peter Kossakowski
kpk@pre-secure.de

Value Added for your Team

- **If you are providing security response or are involved in security crisis management, join the community**
  - requires support by accredited teams
- **If you want to prove your ability to follow best practices and be able to sustain your function, consider to become certified**
  - requires a long term commitment
- **Make sure to liaison with accredited teams in your country regardless!**

TF-CSIRT
Trusted Introducer

For Security Crisis Management

- **TI offers technical, but critical infrastructure support functions**
  - Authenticated
  - Encrypted
  - Robust
  - Out of Band
- **TI maintains the underlying fabric for it**
  - Assessment of teams and maintenance
  - Framework of accepted policies like TLP

Thank you very much for your kind Attention !

https://www.trusted-introducer.org

mailto:ti@trusted-introducer.org

PRESECURE Consulting GmbH
Dr. Klaus-Peter Kossakowski
kpk@pre-secure.de

TF-CSIRT
Trusted Introducer