



TI nine months old

Trusted Introducer
Status report
1 June 2001



Let's assume we all know that ... (i)



- Security is a problem on the Internet
- There's lots of security incidents worldwide
- The police only comes in on a small minority of incidents (for several reasons beyond scope here)



Let's assume we all know that ... (ii)



- There are CSIRTs and ISPs with CSIRT functions dealing with those problems
- There are now a few 100 of those around
- These few 100 CSIRTs have a rough time to find the right CSIRT to tackle ...

CSIRT = Computer Security Incident Response Team
a.k.a. CERT



Let's assume we all know that ... (iii)



- ... and then still they often don't really know whom they are talking to
- So the CSIRT infrastructure is a major problem and becoming worse
- There is no worldwide solution for this yet (FIRST is not, or not yet, ISOC etc are not really involved)



So ...



- The core European CSIRTs decided to start solving that problem among themselves, in Europe, ...
- ... hoping that other regions will join, or copy the effort, or improve on it
- They named their effort

TRUSTED INTRODUCER



TI mission statement



The Trusted Introducer must foster trust and cooperation between CSIRTs in Europe, both new and experienced. The vehicle used to achieve this is to invite CSIRTs to present themselves and describe their service according to an established baseline – thus enabling objectivity, which is regarded as the pre-requisite of trust.





TI process (i)

- The TI registers “known” European CSIRTs as Level 0
- CSIRTs that decide to join the TI framework are invited by the TI to become Level 1
- The Level 1 CSIRT then has 3 months to work together with the TI to present their service according to the TI baseline



TI process (ii)



- If they succeed, the CSIRT is recognized by the TI as Level 2
- Their full baseline presentation is then published in the TI repository with access restricted to Level 2 CSIRTs only
- Contact information and constituency are also published in the public TI repository





TI process (iii)

- Level 2 CSIRTs maintain their status by regularly complying with their baseline presentation – or adapting it when due
- Any non-compliance to the above process results in a fallback to Level 0



TI Level 2 criteria include ... (i)



- Filling out well defined templates



Constituency

Type of constituency (vendor customer base, internal to host organization, ISP customer base, ...)

Description of constituency

Internet domain, AS numbers and/or IP address information describing the constituency

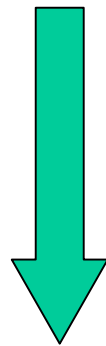
All countries in which constituency members are located in



TI Level 2 criteria include ... (ii)



- Defining information handling policy
- Agreeing to publication of supplied information (only partially in public)



Snapshot of public repository



TRUSTED

Introducer

TI Directory: Level 2 Teams

The TI Process

How to ...

Updates

The Review Board

The TI Team

CSIRT Teams

Links & References

Legal Notice

The following list contains all teams that have successfully acquired level 2 status within Europe at this point in time. *Please note: If your team is listed as level 0 team and you would like to acquire level 2 status, please refer to the appropriate how to step. If you find any error or misrepresentation, we appologize for that and ask you to send us an update.*

- CERT-NL (The Netherlands) entered into Level 2 status on 1. January 2001.
- CSIRT.DK (Danmark) entered into Level 2 status on 20. April 2001.
- GARR-CERT (Italy) entered into Level 2 status on 1. January 2001.
- IRIS-CERT (Spain) entered into Level 2 status
.....

TI Level 2 criteria include ... (iii)



- Regularly maintaining supplied information
- Cooperating with TI in matters above
- Adherence to RFC-2350 recommended
- Visiting FIRST and TF-CSIRT events recommended



TI setup



- Stelvio (www.stelvio.nl) operates TI service
 - Parttime involvement by:
 - Mark Koek
 - Erwan Smits
 - Don Stikvoort (Stelvio CEO)
 - Klaus-Peter Kossakowski (service manager)
- E-mail : ti@stelvio.nl
- Public site : <http://www.ti.terena.nl/>



TI checks and balances (i)



- TERENA focal point to fund service
- TERENA independent (www.terena.nl)
- TERENA experienced in helping setup services, like RIPE NCC
- TI *not* limited to TERENA constituency
- TI Review Board reviews the TI work and deals with special cases and problems



TI checks and balances (ii)



- TI Review Board consists of representatives of Level 2 CSIRTs
- Initially however of well known European network/security individuals:
 - Brian Gilmore, chair (Edinburgh university)
 - Karel Vietsch, secretary (TERENA SG)
 - Andrew Cormack (JANET-CERT)
 - Christoph Graf (SWITCH-CERT)
 - Wilfried Wöber (ACONET)



June 1st 2001 snapshot (i)



- Public website <http://www.ti.terena.nl/>
- 55 CSIRTs registered in repository
- 3 Level 1 CSIRTs:
 - TeliaCERT
 - SI-CERT
 - CERT RENATER



June 1st 2001 snapshot (ii)



- 10 Level 2 CSIRTs

- CERT-NL
- GARR-CERT
- JANET-CERT
- IRIS-CERT
- SIEMENS-CERT
- UniNett CERT
- NORDUNET CERT
- CSIRT.DK
- SBS (BT)
- BTCERTCC

} pioneer teams

- Special repository for only Level 2 CSIRTs available

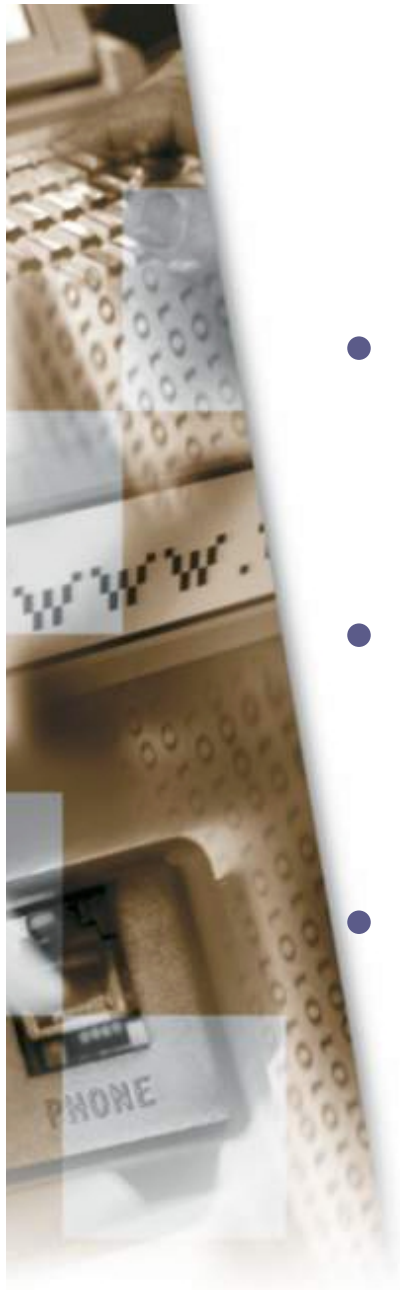


TI does not offer you



- FIRST membership
 - FIRST: only worldwide CSIRT forum
 - FIRST offers nothing like TI yet
 - TI Level 2 CSIRTs are well prepared for FIRST membership
- A free ride
 - Initial fee to go to Level 2 (mainly high level consultancy)
 - Annual Level 2 maintenance cost





TI does offer you

- Public and maintained repository of all “known” or “Level 0” European CSIRTs with contact info
- Formalized and published accreditation process for CSIRTs: those that pass it are “Level 2” CSIRTs --- maintenance is ensured
- Maintained trusted repository for Level 2 CSIRTs only, offering extended information on all members



How to achieve Level 2 ?

(or be registered as Level 0)



- Go to www.ti.terena.nl and follow the logical route OR
- Ask ti@stelvio.nl OR
- Ask any of the TI crew:
 - Mark Koek
 - Erwan Smits
 - Don Stikvoort
 - Klaus-Peter Kossakowski

