Introducing FIRST

Arjen de Landgraaf
CEO Co-Logic Security Ltd (New Zealand), E-Secure-IT
Joint Program Chair FIRST 2007 Annual Conference
arjen.de.landgraaf@cologic.co.nz

Agenda

- Brief bio
- What is FIRST
- Why it was created
- How you join
- Services and benefits
- Questions

Brief Bio

- **E-Secure-IT 1998**

  IT-Security Early Warning and Intelligence

  Four Centres, New Zealand, India, Europe and USA

  www.e-secure-it.com

- **JPC FIRST 2007 Annual Conference,**

17 – 22 June 2007, Sevilla, Spain

What is FIRST?

http://www.first.org/

- **Only worldwide CSIRT forum**
  - Premier organization and recognized global leader in incident response. Membership in FIRST enables incident response teams to more effectively respond to security incidents - reactive as well as proactive.
- **Official recognition from The United Nations as a Non-Governmental Organization (NGO)**

The creation of FIRST

- **"There may be a virus loose on the internet."**
  - Andy Sudduth, 00.34 November 3rd 1988
  - 10% of the Internet taken down (60,000 of 600,000 hosts)
- **DARPA post mortem, November 8th 1988**
  - Worm analysed quickly, but:
    - Lack of communication
    - Coordination and research of incidents needed
- **CERT created at SEI/CMU, Pittsburgh, November 17th 1988**
  - http://www.cert.org/

FIRST™ Improving Security Together

The creation of FIRST (Cont.)

- **WANK and OILZ worms infect DECNET – October 1989**
  - CERT, CIAC and NASA teams research and issue warnings
  - US National Academy report, Computers at Risk: Safe Computing in the Information Age, calls for development of CSIRTs and international harmonization of efforts, mid-1990

- **FIRST founded - November 1990**
  - 10 members from the US, 1 from Europe
    - Air Force Computer Emergency Response Team (AFCERT)
    - CERT(sm) Coordination Center (CERT/CC)
    - Defense Communication Agency/Defense Data Network (DCA/DDN)
    - Department of Army Response Team
    - Department of Energy's Computer Incident Advisory Capability, Lawrence Livermore National Laboratory (DOE's CIAC)
    - Goddard Space Flight Center
    - NASA Ames Research Center Computer Network Security Response Team (NASA ARC CNSRT)
    - NASA Space Physics Analysis Network (SPAN CERT)
    - Naval Computer Incident Response Team (NAVCIRT)
    - National Institute of Standards and Technology Computer Security Resource and Response Center (CSRC)
    - SPAN-France

Vision

FIRST is a premier organization and recognized global leader in incident response.

Membership in FIRST enables incident response teams to more effectively respond to security incidents by providing access to best practices, tools, and trusted communication with member teams.

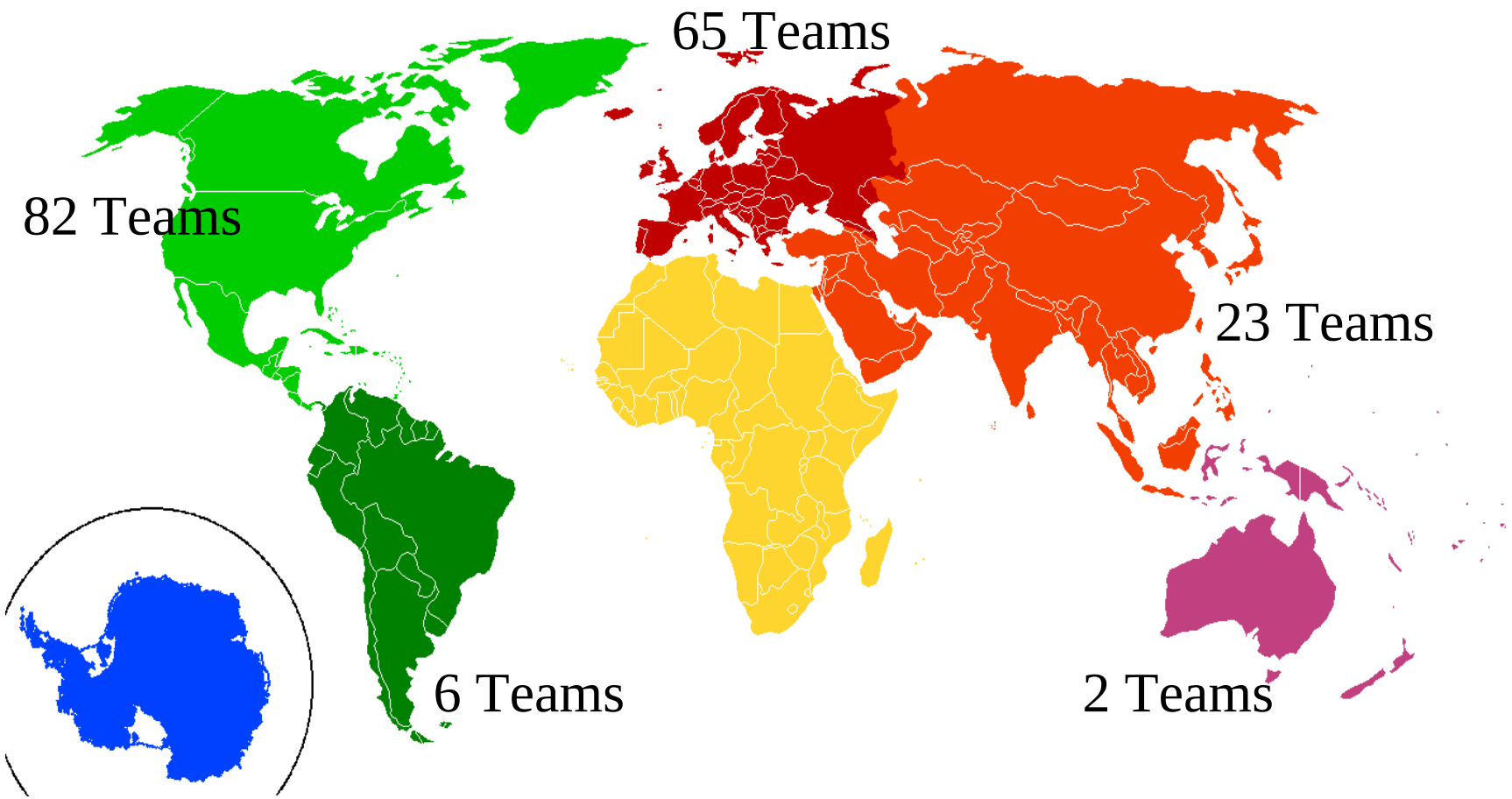
Mission

FIRST is an international confederation of trusted computer incident response teams who cooperatively handle computer security incidents and promote incident prevention programs.

- FIRST members develop and share technical information, tools, methodologies, processes and best practices
- FIRST encourages and promotes the development of quality security products, policies & services
- FIRST develops and promulgates best computer security practices
- FIRST promotes the creation and expansion of Incident Response teams and membership from organizations around the world
- FIRST members use their combined knowledge, skills and experience to promote a safer and more secure global electronic environment

Geographical Coverage

May 2006



FIRST™
Improving Security Together

Services and benefits

VDF and CVSS

- **Common Vulnerability Scoring System**
  - A rating system designed to provide open and universally standard severity ratings of software vulnerabilities (NIAC report Jan 2005)
- **Vulnerability Disclosure Framework**
  - National Infrastructure Advisory Council (NIAC) working group report (Jan 2004)
    - http://www.dhs.gov/interweb/assetlibrary/vdwgreport.pdf
  - Defines roles and expectations
- **FIRST is steward of CVSS and is striving for widespread adoption of the VDF**

Law Enforcement and FIRST

- Numerous government teams among FIRST members – but law enforcement thus far under represented
- June 2005 decision to encourage law enforcement membership
- Focus on open information exchange
- First FIRST Law Enforcement member November 2005. (National Police Agency, CFC – Cyber Force Center, JP)
- Special Law Enforcement & CSIRT workshop at the 2007 Sevilla conference

SIG's (Special Interest Groups)

- Abuse Handling (AH) SIG
- Artefact Analysis (AA) SIG
- Common Vulnerabilities Score Systems (CVSS) SIG
- Internet Infrastructure Vendors (IIV) SIG
- Law Enforcement/CSIRT Cooperation (LE-CC) SIG
- Network Monitoring (NM) SIG
- Phishing SIG
- Etc.

FIRST™
Improving Security Together

Corporate Executive Programme (CEP)

- Bring together cross-functional senior executives with responsibility for decision-making in their organisations.
- The Programme caters for heads of departments in HR, Finance, Operations, Technology, Security, Sales & Marketing, Research, Logistics, Legal and other key business disciplines in all sectors – public and private – across all global regions.

- http://www.globalcep.com

Other FIRST Resources

- **Mailing Lists**
- **Web Site**
  - Best Practice Guides
  - Team Contact details
  - Presentations
- **Regional TC's (Technical Colloquia)**
- **Training**
  - (TRANSITS: Training of Network Security Incident Teams Staff)
    - Session at Sevilla 2007 Conference

FIRST Education

The mission of the FIRST Education Committee is to ensure that high-quality, affordable education and training is available to those who wish to create or operate incident response teams that further the goals and objectives of FIRST. This mission derives directly from the FIRST Mission Statement. **Work Programme**

1. Stimulate and support regular CSIRT training courses in the various regions of the world (currently FIRST uses the TRANSITS courses as a vehicle for this, in cooperation with TERENA) - this includes "training the trainers" in special T3 courses
2. Provide regular "hands-on classes" as part of FIRST Technical Colloquia or special events like joint workshops
3. Develop new training tools, courses and techniques for the good of the FIRST membership
4. Help newly arrived CSIRTs develop by training, and stimulate them to join FIRST

FIRST Education (Cont.)

Support/provision of TRANSITS Training Courses - at least once per year in Europe, AP and LA regions - supported by FSS

Train-the-trainer courses - once a year at the FIRST conference - organized by the Education Committee

TRANSITS materials in several languages (English, Spanish, Chinese) - supported by FSS

Hands-on classes - organized by Jacomo Piccolini (CAIS)

Leveraging Membership

- **Phishing**
  - Able to leverage response teams around the world to take down sites
  - China & South Korea especially useful
- **Worms and Botnets**
- **Advisories and Vulnerability Handling**
- **SIG**
- **Reliable expert knowledge**

FIRST™
Improving Security Together

How do you join FIRST?

- **Membership Levels**
  - Full
  - Liaison
- **Sponsors – Two FULL member sponsors**
- **Site Visit**
- **Paperwork**
- **Steering Committee vote**
  - Requires 2/3 affirmative vote
- **http://www.first.org/membership/process.html**

FIRST Events

FIRST™
Improving Security Together

19th Annual FIRST Conference

- June 17 - 22, 2007 in Sevilla, Spain
- Learn the latest security strategies and solutions
- Keep up-to-date with the latest incident response and prevention techniques
- Gain insight into analyzing system and network vulnerabilities
- Meet colleagues from around the world and exchange ideas and advice

FIRST™
Improving Security Together

FIRST 2007 Annual Conference

- Theme: Private Lives and Corporate Risk
- The five-day event is comprised of two days of tutorials and three days of technical sessions where a range of topics of interest to teams in this global response community will be discussed.

FIRST™
Improving Security Together

FIRST 2007 Special Events

- Dinner
- Best Presentation Awards
- Beer 'n Gear
- Security Challenge
- *Lightning Talks*
- Birds-of-a-Feather Sessions
- Train the Trainers Workshop (3T)
- Special Workshops
- SIG Meetings
- PGP Key Signing Service
- Elevator Pitches
- Vendor Exhibition

FIRST 2007 Annual Conference

http://www.first.org/conference/2007/

Questions?

Contact Information

www: http://www.first.org/

Email: first-2007@first.org

Improving Security Together