Incident Management and Computer Security Incident Response Teams (CSIRTs)

Slides available at: http://www.cert.br/docs/presentations/

Cristine Hoepers
General Manager
<cristine@cert.br>

CERT.br – CERT Brazil
http://www.cert.br/

NIC.br – Brazilian Network Information Center
http://www.nic.br/
CGI.br – Brazilian Internet Steering Committee
http://www.cgi.br/

Agenda

- Background about CERT.br / NIC.br / CGI.br
- Introduction / Historical Perspective
  - Definition of CSIRT
  - Beginning of Incident Response and CSIRTs
  - How it evolved in Brazil
- Incident Management and CSIRTs
  - Definition of Incident Management
  - Incident Management, Handling and Response
- Additional Information
  - CSIRTs with national responsibility
  - Regional Initiatives
  - Proactive services
- Resources

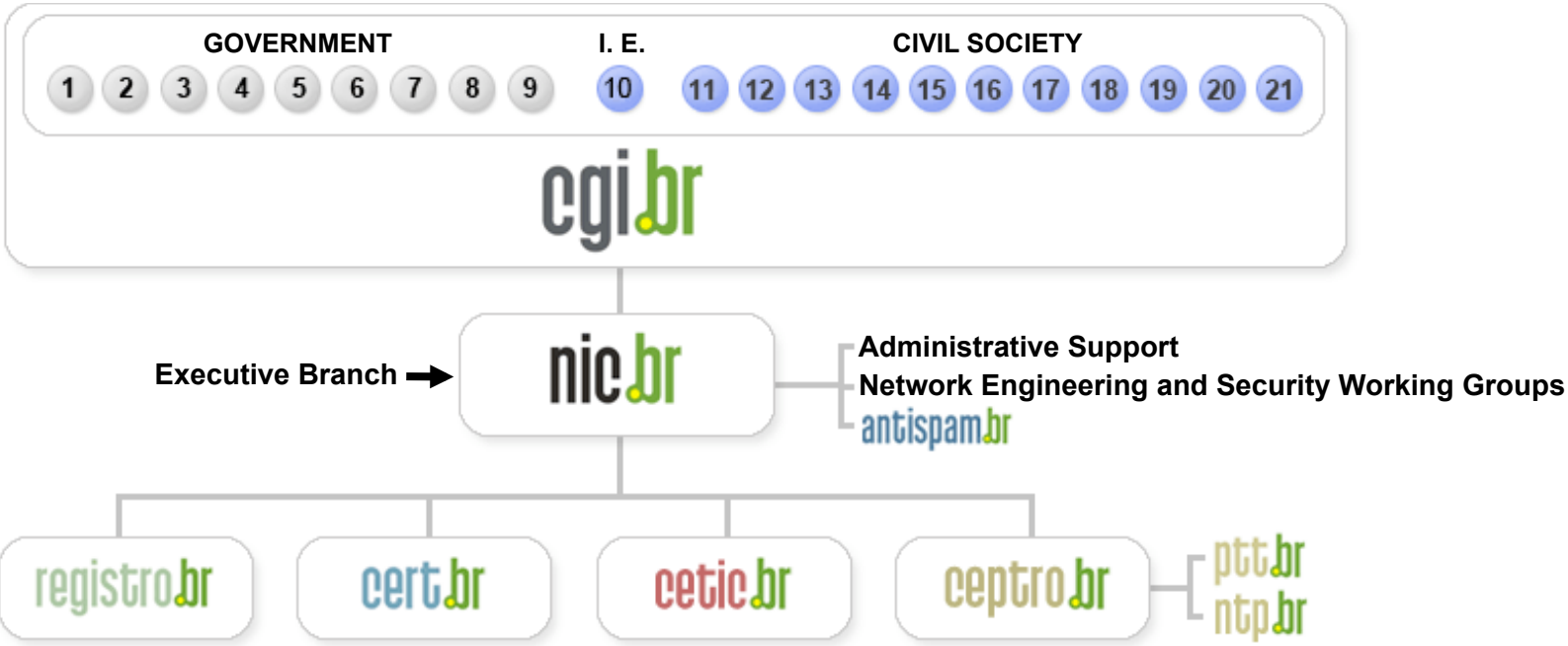
Brazilian Internet Governance

Brazilian Internet Steering Committee – CGI.br – is a multi-stakeholder organization created in 1995 that among diverse responsibilities has these main attributions:

- to propose policies and procedures related to the regulation of Internet activities
- **to recommend standards for technical and operational procedures**
- to establish strategic directives related to the use and development of Internet in Brazil
- **to promote studies and technical standards for the network and services' security in the country**
- to coordinate the allocation of Internet addresses (IP) and the registration of domain names using <.br>
- **to collect, organize and disseminate information on Internet services, including indicators and statistics**

http://www.cgi.br/internacional/

CGI.br and NIC.br Structure

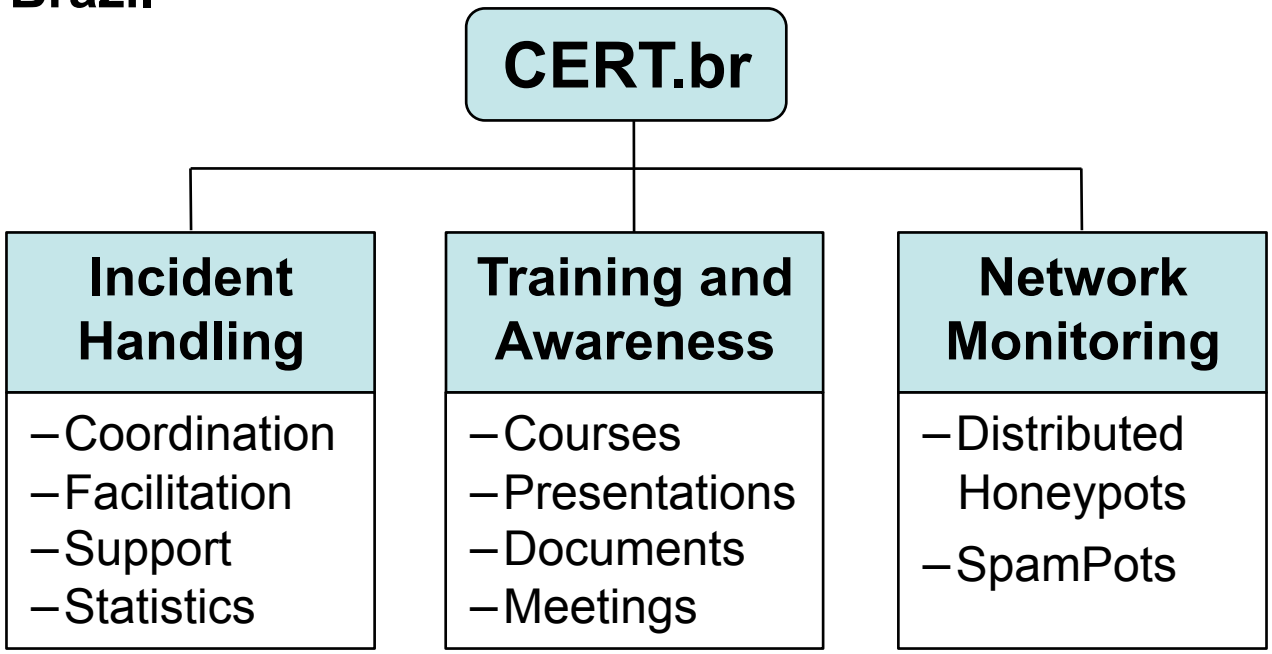


1 – Ministry of Science and Technology (Coordination)
2 – Ministry of Communications
3 – Presidential Cabinet
4 – Ministry of Defense
5 – Ministry of Development, Industry and Foreign Trade
6 – Ministry of Planning, Budget and Management
7 – National Telecommunications Agency
8 – National Council of Scientific and Technological Development
9 – National Forum of Estate Science and Technology Secretaries
10 – Internet Expert

11 – Internet Service Providers
12 – Telecommunication Infrastructure Providers
13 – Hardware and Software Industries
14 – General Business Sector Users
15 – Non-governmental Entity
16 – Non-governmental Entity
17 – Non-governmental Entity
18 – Non-governmental Entity
19 – Academia
20 – Academia
21 – Academia

CERT.br Activities

Created in 1997 as the national focal point to handle computer security incident reports and activities related to networks connected to the Internet in Brazil



International Partnerships

FIRST Improving Security Together MEMBER

Anti-Phishing Working Group APWG

SEIPartner CERT Courses

The Honeynet PROJECT®

Introduction / Historical Perspective

What is a CSIRT?

A CSIRT is a concrete organizational entity (i.e., one or more staff) that is assigned the responsibility of providing part of the incident management capability for a particular constituency.

CSIRTs provide – at a minimum – incident handling activities, which include:

- **determining the impact, scope, and nature of the event or incident**
- **understanding the technical cause of the event or incident**
- **researching and recommending solutions and workarounds**
- **coordinating and supporting the implementation of the response strategies with other parts of the enterprise or constituency**
- **disseminating information on current risks, threats, attacks, exploits, and corresponding mitigation strategies through alerts, advisories, Web pages, and other technical publications**
- **coordinating and collaborating with external parties such as vendors, ISPs, other security groups and CSIRTs, and law enforcement**

Source: Defining Computer Security Incident Response Teams.
https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/incident/662-BSI.html

CSIRT Acronyms and Names

CSIRT	Computer Security Incident Response Team
CSIRC	Computer Security Incident Response Capability
CIRC	Computer Incident Response Capability
CIRT	Computer Incident Response Team
IHT	Incident Handling Team
IRC	Incident Response Center or Incident Response Capability
IRT	Incident Response Team
SERT	Security Emergency Response Team
SIRT	Security Incident Response Team

CERT® "CERT" and "CERT Coordination Center" are registered with the U.S. Patent and Trademark office as service marks of Carnegie Mellon University.

- New teams should not expand the acronym
- Organizations that wish to use the CERT mark in their name must ask permission – send an email to **cert@cert.org**
  http://www.cert.org/csirts/csirt_faq.html

Early Years

- **1988**
  - **November 2: Internet (Morris) Worm**
  - **November 8: *Post Mortem* meeting**
  - **November 17: CERT/CC Created**
- **1989**
  - **October: first invitational workshop organized by CERT/CC**
- **1990**
  - **October: second workshop – talks about creating a Forum of International Teams**
  - **November: 11 Teams created a Forum of CSIRTs, which is now FIRST – Forum of Incident Response and Security Teams (http://www.first.org/)**
- **1991–1992**
  - **European research networks started the first teams: SURFnet and DFN**
- **1993**
  - **The first CSIRT was created in Asia-Pacific: AusCERT**

Source: State of the Practice of Computer Security Incident Response Teams.
http://www.cert.org/archive/pdf/03tr001.pdf

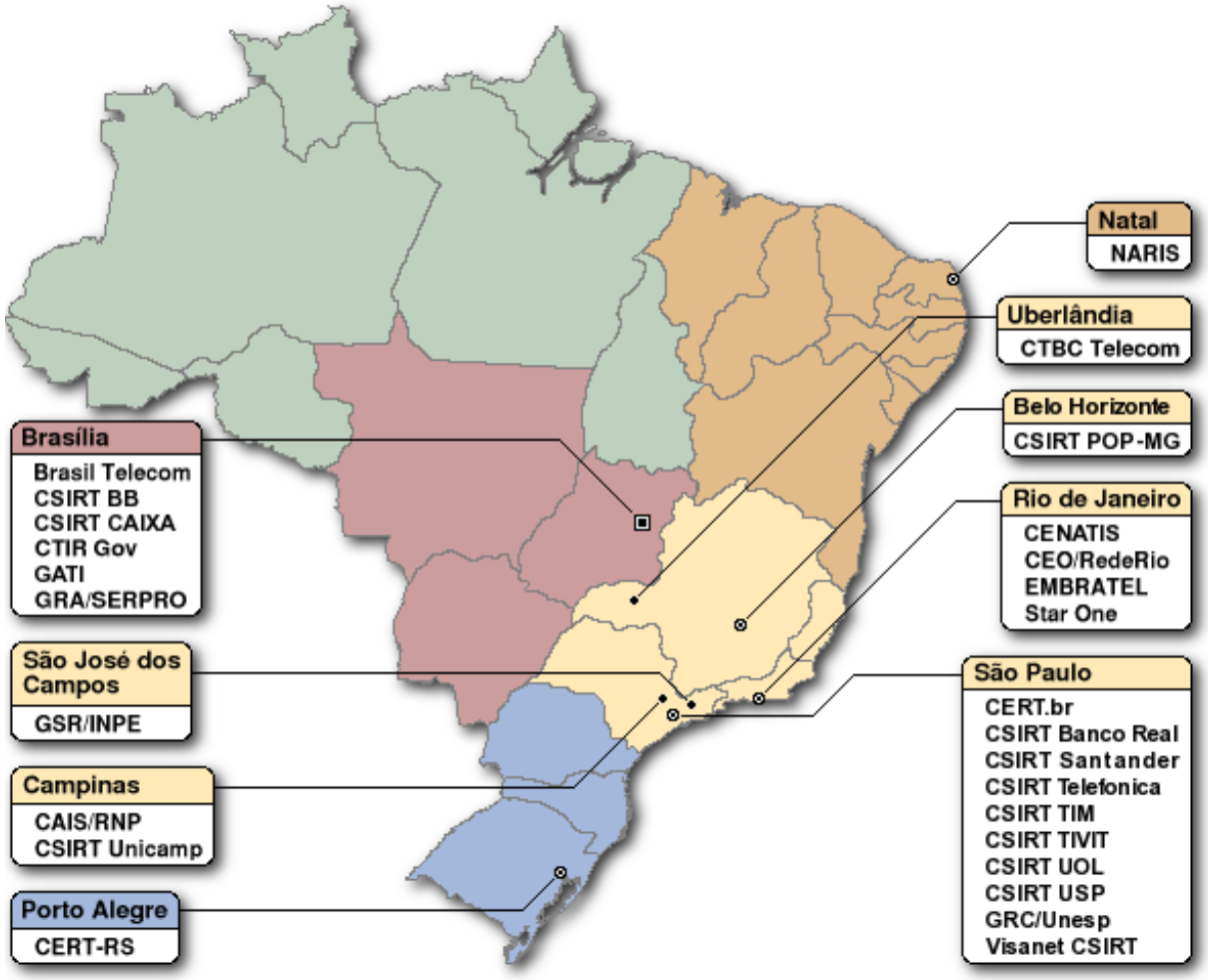
Development of Incident Handling in Brazil

- August/1996: CGI.br released the document: “Towards the Creation of a Security Coordination Center for the Brazilian Internet.”[1]
- June/1997: CGI.br created CERT.br (at that time called NBSO), as the CSIRT with national responsibility, based on the report's recommendation[2]
- August/1997: the Brazilian Research Network (RNP) created it’s own CSIRT (CAIS)[3], followed by the Rio Grande do Sul Academic Network CERT-RS[4]
- 1999: other institutions, including Universities and Telecommunication Companies started forming their CSIRTs
- 2003/2004: task force to discuss the structure of a CSIRT for the Federal Government Administration
- 2004: CTIR Gov was created, with the Brazilian Federal Government Administration as their constituency[5]

[1] http://www.nic.br/grupo/historico-gts.htm
[2] http://www.nic.br/grupo/gts.htm
[3] http://www.rnp.br/_arquivo/documentos/rel-rnp98.pdf
[4] http://www.cert-rs.tche.br/cert-rs.html
[5] http://www.ctir.gov.br/

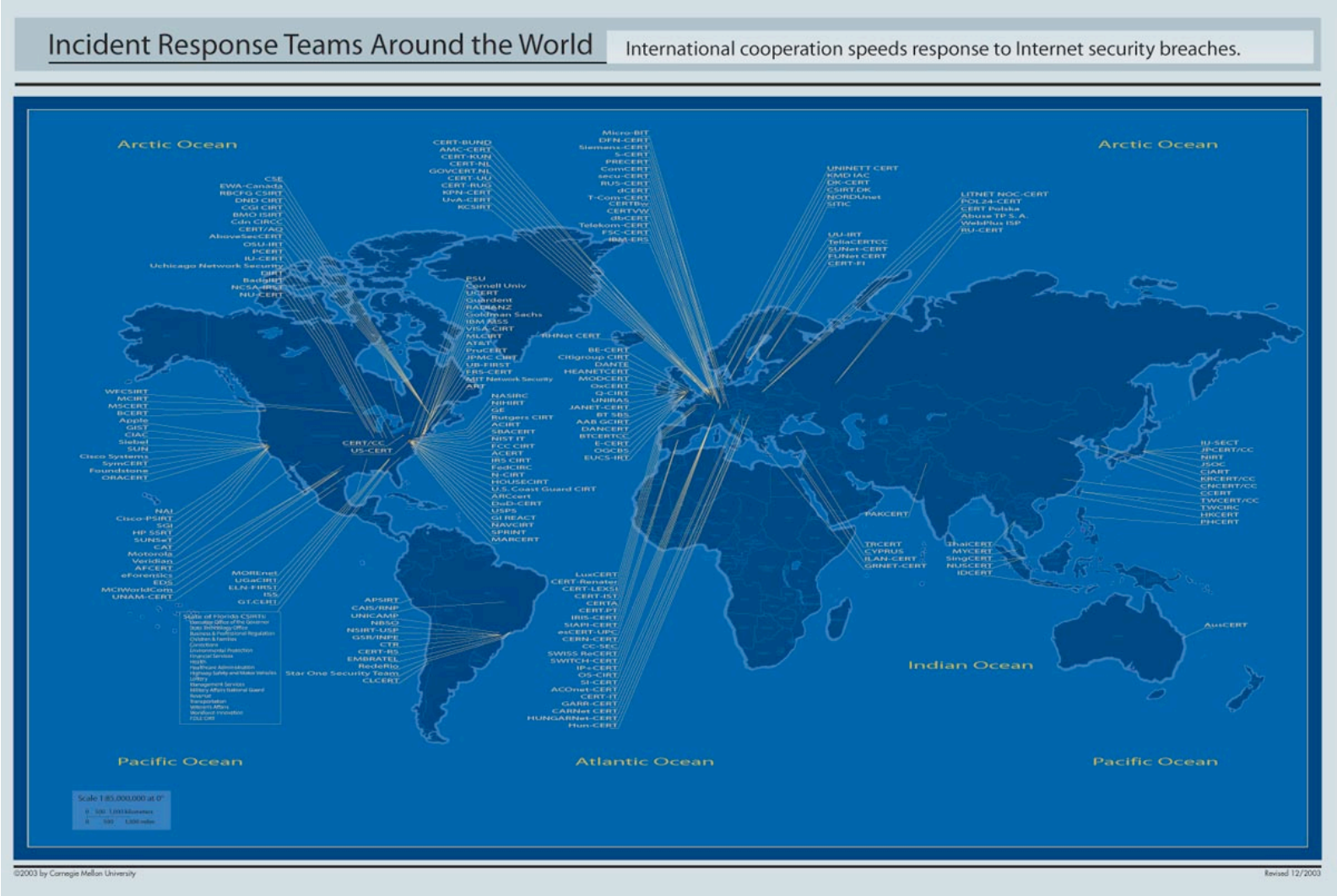
CSIRTs in Brazil

Sector	CSIRTs
National Responsibility	CERT.br
Government Networks	CTIR Gov, GATI, GRA/SERPRO
Financial Sector	CSIRT BB, CSIRT CAIXA, CSIRT Banco Real, CSIRT Santander, Visanet CSIRT
Telecom/ISP	Brasil Telecom, CTBC Telecom, EMBRATEL, StarOne, CSIRT Telefonica, CSIRT TIM, CSIRT UOL
Academic and Research Networks	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CENATIS, CEO/RedeRio, CSIRT USP, GRC.UNESP
Outsourcing	CSIRT TIVIT



http://www.cert.br/contact-br.html

CSIRTs Around the Globe



Source: CERT Coordination Center
http://www.cert.org/csirts/csirt-map.html

Incident Management and CSIRTs

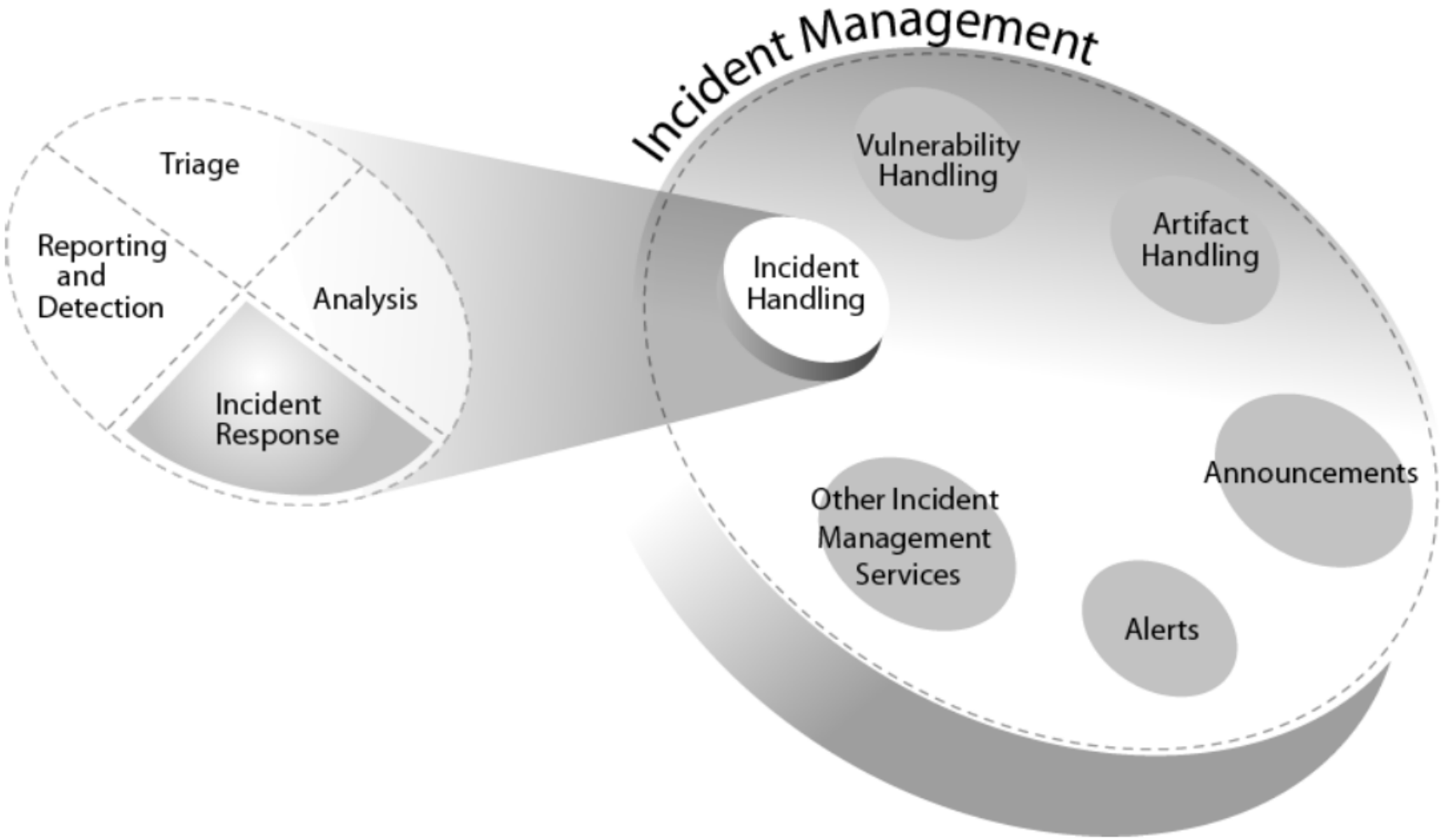
Incident Management

The ability to provide management of computer security events and incidents. It implies end-to-end management for controlling or directing how security events and incidents should be handled. It involves:

- **defining a process to follow with supporting policies and procedures in place**
- **assigning roles and responsibilities**
- **having appropriate equipment, infrastructure, tools, and supporting materials ready**
- **having qualified staff identified and trained to perform the work in a consistent, high-quality, and repeatable way**

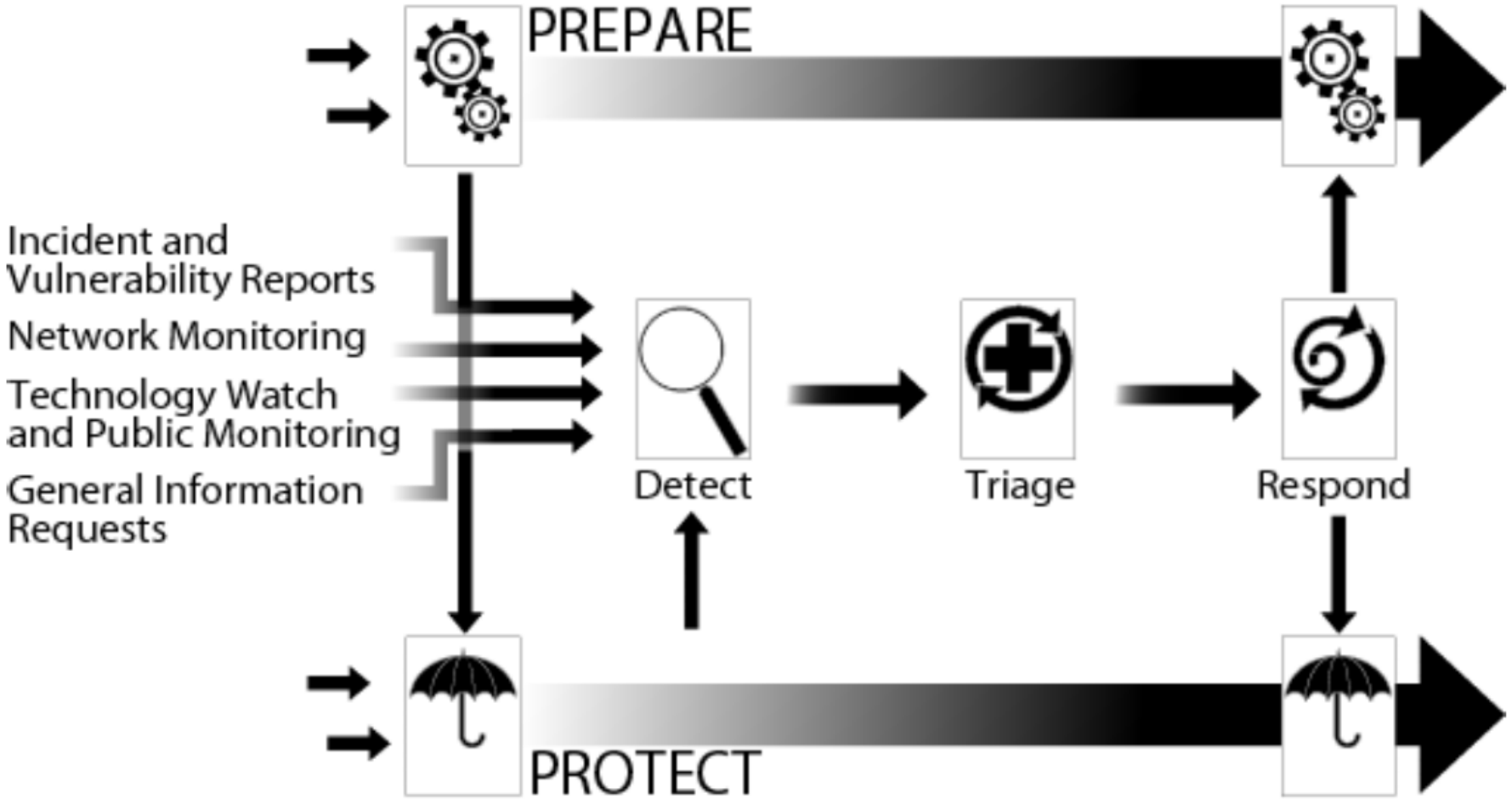
Source: Incident Management.
https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/incident/223-BSI.html

Incident Management, Handling and Response



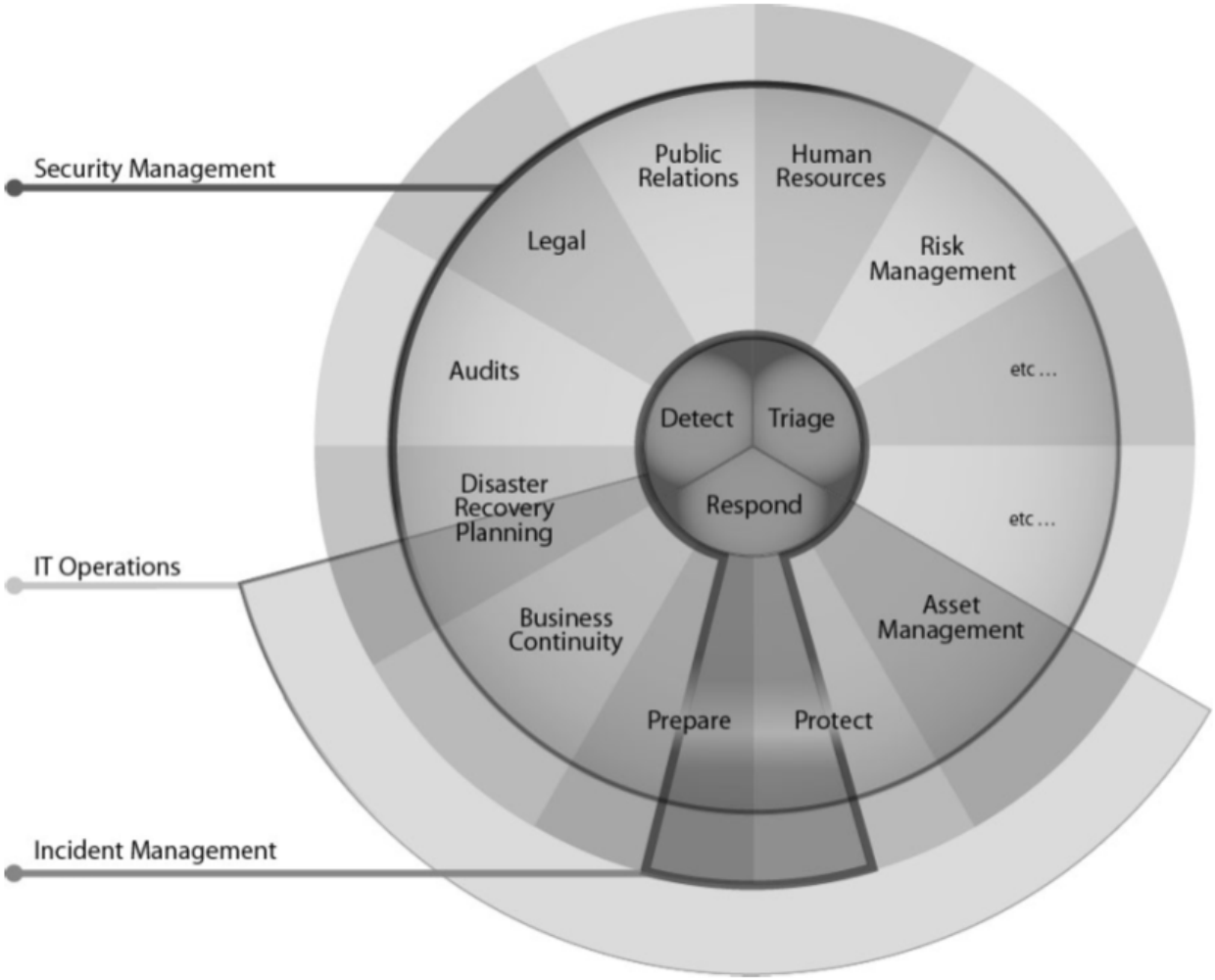
Source: Defining Incident Management Processes for CSIRTs: A Work in Progress.
Picture used with permission from CERT Program and SEI/CMU.
http://www.cert.org/archive/pdf/04tr015.pdf

Relationship Between Processes



Source: Defining Incident Management Processes for CSIRTs: A Work in Progress.
Picture used with permission from CERT Program and SEI/CMU.
http://www.cert.org/archive/pdf/04tr015.pdf

IT Operations, Security and Incident Management



Source: Defining Incident Management Processes for CSIRTs: A Work in Progress.
Picture used with permission from CERT Program and SEI/CMU.
http://www.cert.org/archive/pdf/04tr015.pdf

Possible CSIRT Services

Reactive Services

- Alerts and Warnings
- Incident Handling
  - Incident analysis
  - Incident response on site
  - Incident response support
  - Incident response coordination
- Vulnerability Handling
  - Vulnerability analysis
  - Vulnerability response
  - Vulnerability response coordination
- Artifact Handling
  - Artifact analysis
  - Artifact response
  - Artifact response coordination

Proactive Services

- Announcements
- Technology Watch
- Security Audit or Assessments
- Configuration & Maintenance of Security Tools, Applications, & Infrastructures
- Development of Security Tools
- Intrusion Detection Services
- Security-Related Information Dissemination

Security Quality Management Services

- ✓ Risk Analysis
- ✓ Business Continuity & Disaster Recovery Planning
- ✓ Security Consulting
- ✓ Awareness Building
- ✓ Education/Training
- ✓ Product Evaluation or Certification

Source: Defining Incident Management Processes for CSIRTs: A Work in Progress.
Picture used with permission from CERT Program and SEI/CMU.
http://www.cert.org/archive/pdf/04tr015.pdf

Choosing Services

Incident Handling is the core service – but could vary from incident analysis and support to incident response on site

Other services are usually chosen according to:

- **needs of the constituency**
- **expertise of team members**

Services being provided can change and evolve to accommodate:

- **new threats**
- **changes in the constituency's use of the Internet**
- **change of scope in threats**
- **new demands from the constituency**

It is important to start small and grow over time

Action List for Creating a CSIRT

1. Identify stakeholders and participants
2. Obtain management support and sponsorship
3. Develop a CSIRT Project Plan
4. Gather information
5. Identify the CSIRT constituency
6. Define the CSIRT mission
7. Secure Funding for CSIRT operations
8. Decide on the range and level of services the CSIRT will offer
9. Determine the CSIRT reporting structure, authority, and organizational model
10. Identify required resources such as staff, equipment, and infrastructure
11. Define interactions and interfaces
12. Define roles, responsibilities, and the corresponding authority
13. Document the workflow
14. Develop policies and corresponding procedures
15. Create an implementation plan and solicit feedback
16. Announce the CSIRT when it becomes operational
17. Define methods for evaluating the performance of the CSIRT
18. Have a backup plan for every element of the CSIRT
19. Be flexible

http://www.cert.org/csirts/action_list.html

Additional Information

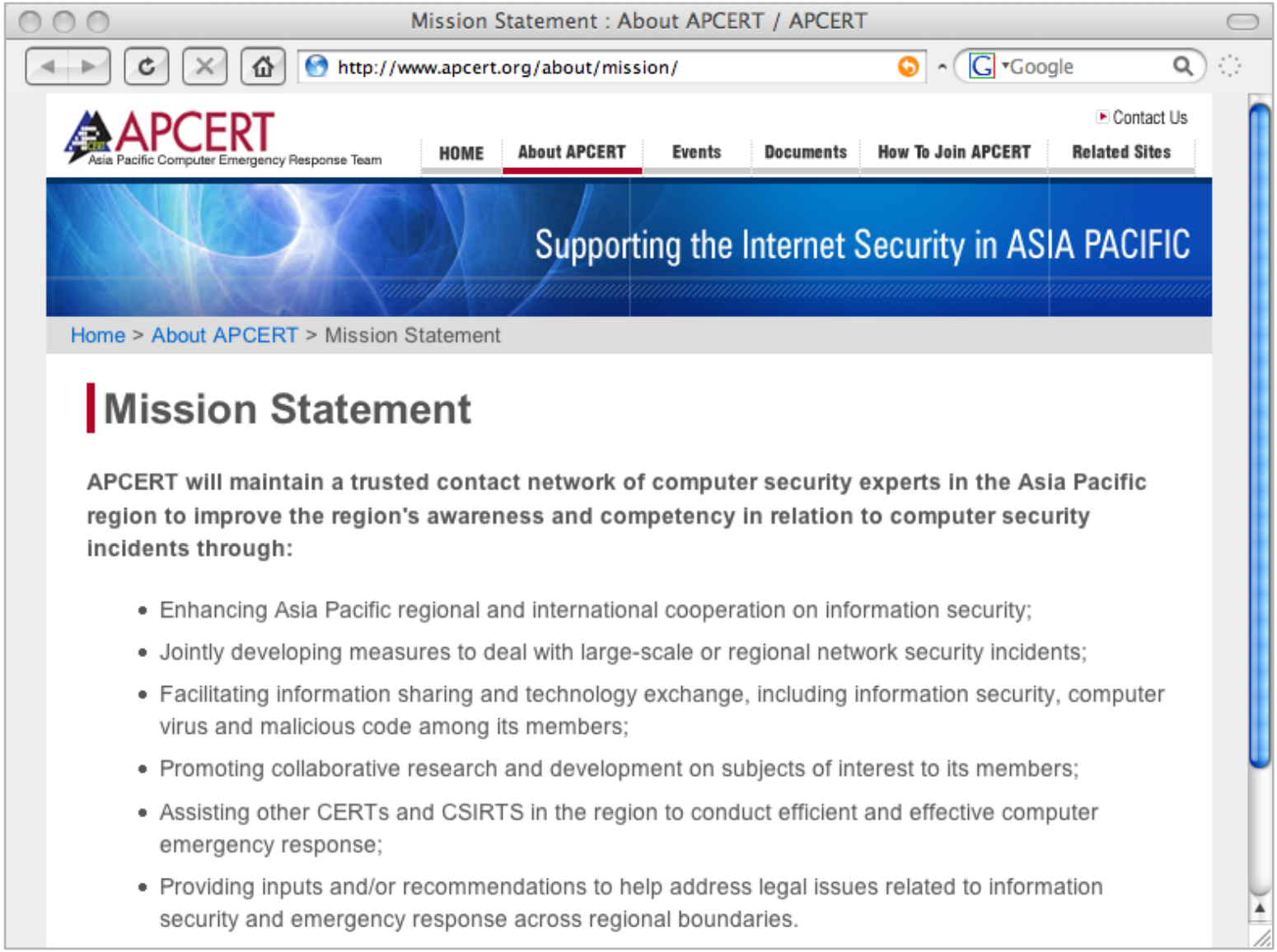
CSIRTs with National Responsibility

Have responsibility over an economy or a country

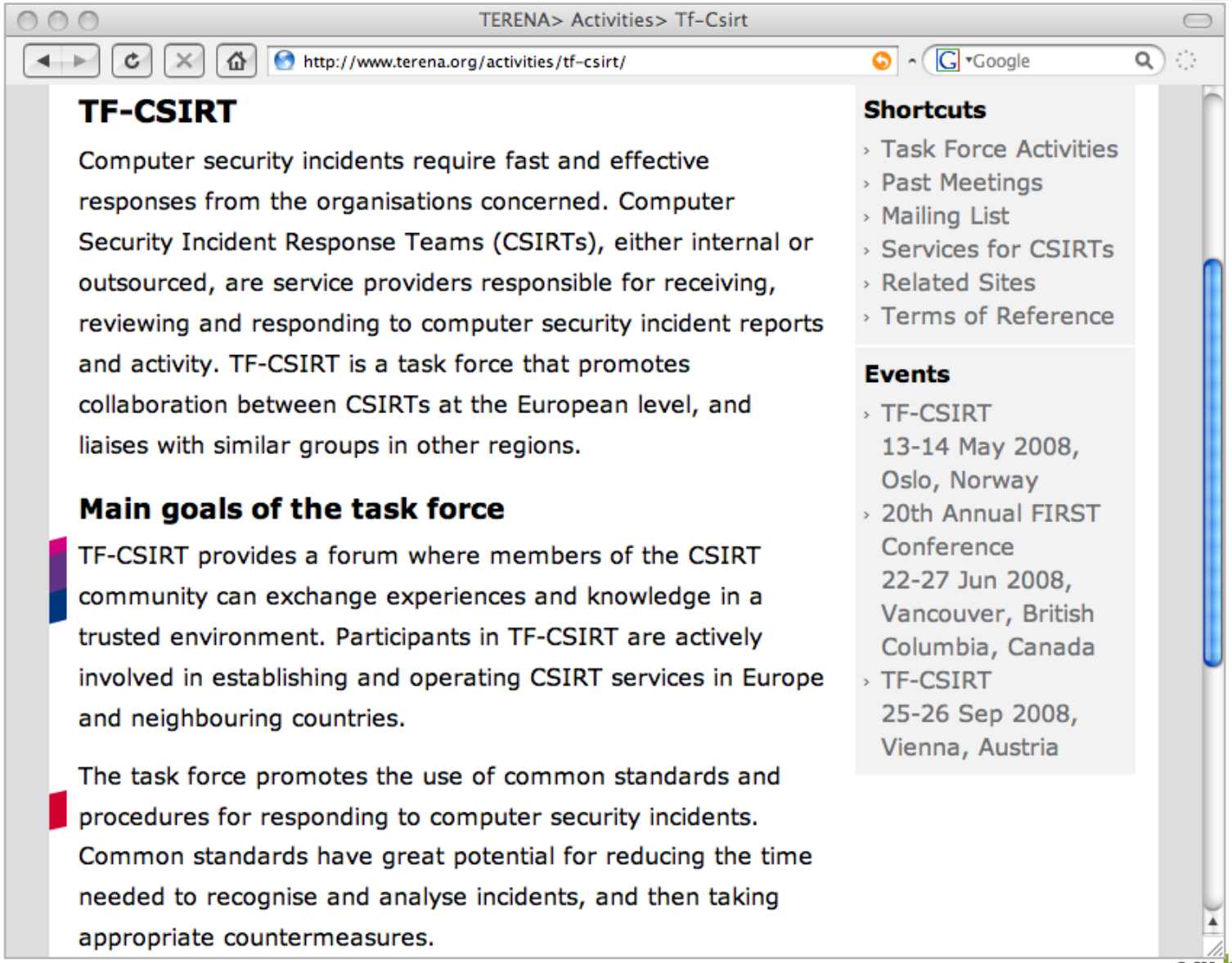
- Their constituencies vary
  - All networks
  - General public
  - Governmental networks
  - Critical Infrastructure
  - A combination of the above
- Often operate as "teams of last resort" in their country
- List of national CSIRTs and information about meetings and cooperation among national teams

  http://www.cert.org/csirts/national/

APCERT – http://www.apcert.org/



TF-CSIRT – http://www.terena.org/activities/tf-csirt/



ECG – http://www.bsi.de/certbund/EGC/index_en.htm

Membership European Government CERTs (EGC) group

The European Government CSIRTs group (EGC) is an informal group of governmental CSIRTs that is developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe.

To achieve this goal, the EGC group members will:

- Jointly develop measures to deal with large-scale or regional network security incidents
- Facilitate information sharing and technology exchange relating to IT security incidents and malicious code threats and vulnerabilities
- Identify areas of specialist knowledge and expertise that could be shared within the group
- Identify areas of collaborative research and development on subjects of mutual interest
- Encourage formation of government CSIRTs in European countries
- Communicate common views with other initiatives and organizations.

Current members of the European Government CSIRTs group:

- Finland – CERT-FI
- France – CERTA
- Germany – CERT-Bund
- Hungary – CERT-Hungary
- The Netherlands – GOVCERT.NL
- Norway – NorCERT
- Sweden – SITIC
- United Kingdom – CSIRTUK
- United Kingdom - GovCertUK

GCC-CERT – http://www.ict.gov.qa/output/NewsPage.aspx?PageID=752

GCC-CERT Center discussed

http://www.ict.gov.qa/output/NewsPage.aspx?PageID=

Google

GCC-CERT Center discussed

ictQATAR promotes information security regionally

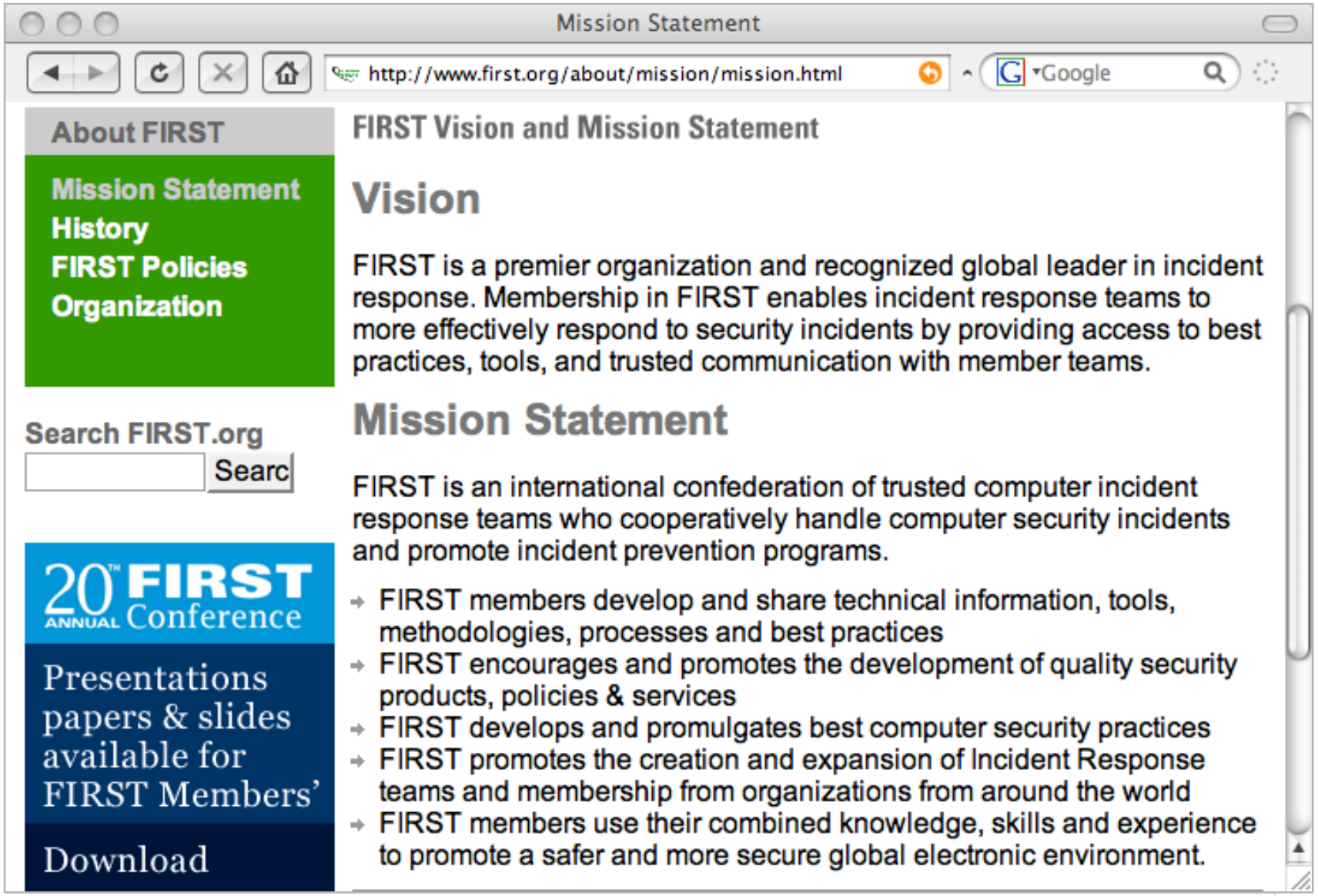
Doha, Qatar (16 June 2008): The Supreme Council for Information & Communications Technology, ictQATAR hosted a one-day meeting yesterday at Sharq Village and Spa for the GCC - CERT Directors and Information Security officials to discuss key initiatives on information security.

The meeting is an outcome of one of the recommendations of the GCC Ministerial Meeting for Post, Communications & Information Technology held last month in Doha to establish a GCC-CERT committee.

GCC-CERT Center discussed

During the meeting, GCC-CERT officials and Qatar's Center for Information Security

FIRST – http://www.first.org/



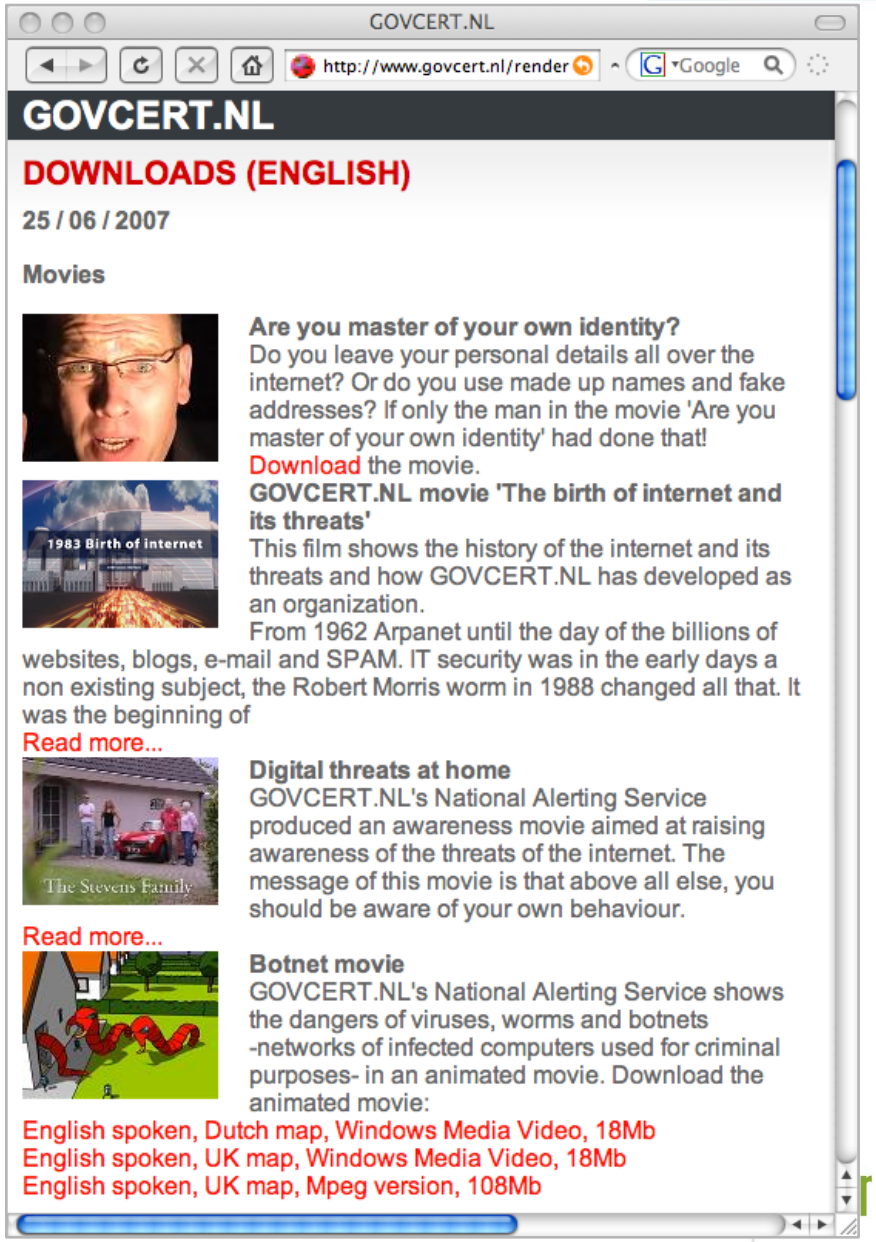
Proactive Services (1/3)

- More and more teams are focusing in awareness, prevention and network monitoring, partially as a result from
  - Botnet and Fast Flux networks
  - Attacks targetted at the end users
- Network monitoring projects examples:
  - SURFnet & GOVCERT.NL: SURFids
    http://ids.surfnet.nl/
  - NASK/CERT-Polska & GOVCERT.NL & SURFnet: HoneySpider Network
    http://www.honeyspider.org/
  - CERT-Polska: ARAKIS
    http://www.arakis.pl/
  - JPCERT/CC: Internet Scan Data Acquisition System (ISDAS) Project
    http://www.jpcert.or.jp/isdas/index-en.html
  - CERT.br: Brazilian Distributed Honeypots; and The SpamPots Project
  - CERT.br and other National CSIRTs: SpamPots – International Phase

Proactive Services (2/3)

End users awareness

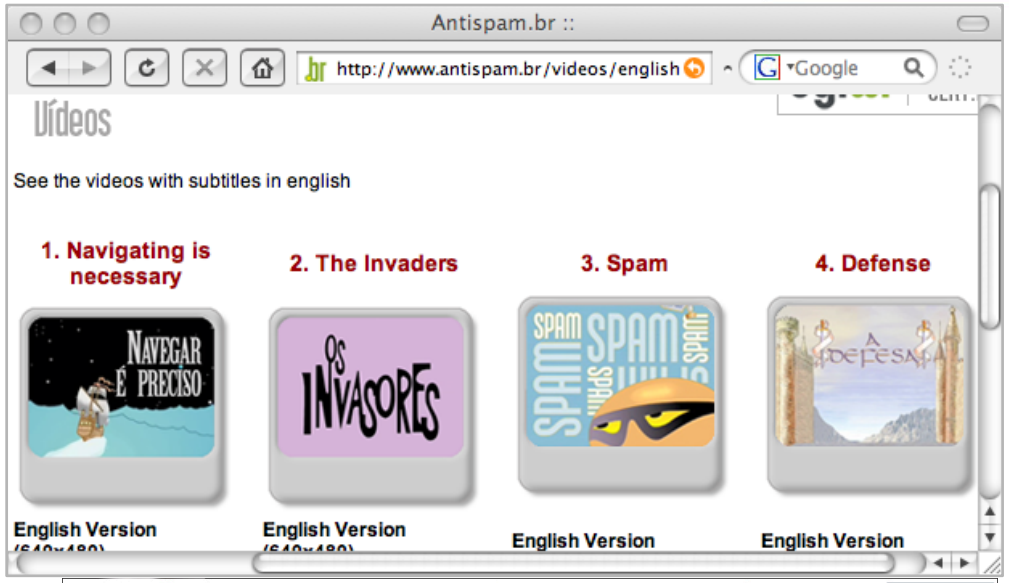
- GOVCERT.NL
  - Movies
    - identity theft
    - threats
    - end user behaviour
    - botnets & worms
  - Alerting service



Proactive Services (3/3)

End users awareness

- CERT.br
  - Antispam.br content
    - Website
      http://www.antispam.br/
    - Videos / Characters
  - Best practices
    - Website
      http://www.cartilha.cert.br/
    - Book & tips folder



Resources

Resources for CSIRTs (1/2)

- **Creating a Computer Security Incident Response Team: A Process for Getting Started**
  http://www.cert.org/csirts/Creating-A-CSIRT.html
- **CSIRT Services**
  http://www.cert.org/csirts/services.html
- **State of the Practice for CSIRTs**
  http://www.cert.org/archive/pdf/03tr001.pdf
- **Defining Incident Management Processes**
  http://www.cert.org/archive/pdf/04tr015.pdf
- **Staffing Your CSIRT**
  http://www.cert.org/csirts/csirt-staffing.html
- **Steps for Creating National CSIRTs**
  http://www.cert.org/archive/pdf/NationalCSIRTs.pdf

Resources for CSIRTs (2/2)

- **Handbook for Computer Security Incident Response Teams**
  http://www.cert.org/archive/pdf/csirt-handbook.pdf
- **Organizational Models for CSIRTs**
  http://www.cert.org/archive/pdf/03hb001.pdf
- **Other CSIRT Related documents**
  http://www.cert.org/csirts/
- **Training**
  CERT Program – http://www.cert.org/training/
  AusCERT – http://www.auscert.org.au/render.html?cid=1934
  CERT.br (CERT Program content) – http://www.cert.br/cursos/
- **Resources in Portuguese**
  http://www.cert.br/csirts/

Thank you for your attention

Slides available at: http://www.cert.br/docs/presentations/

Cristine Hoepers
General Manager
<cristine@cert.br>

CERT.br – CERT Brazil
http://www.cert.br/

NIC.br – Brazilian Network Information Center
http://www.nic.br/
CGI.br – Brazilian Internet Steering Committee
http://www.cgi.br/