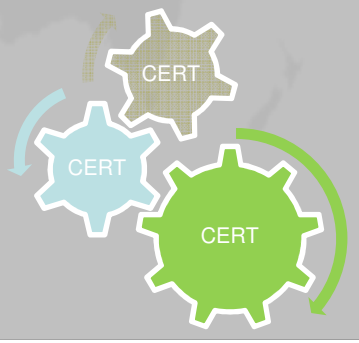
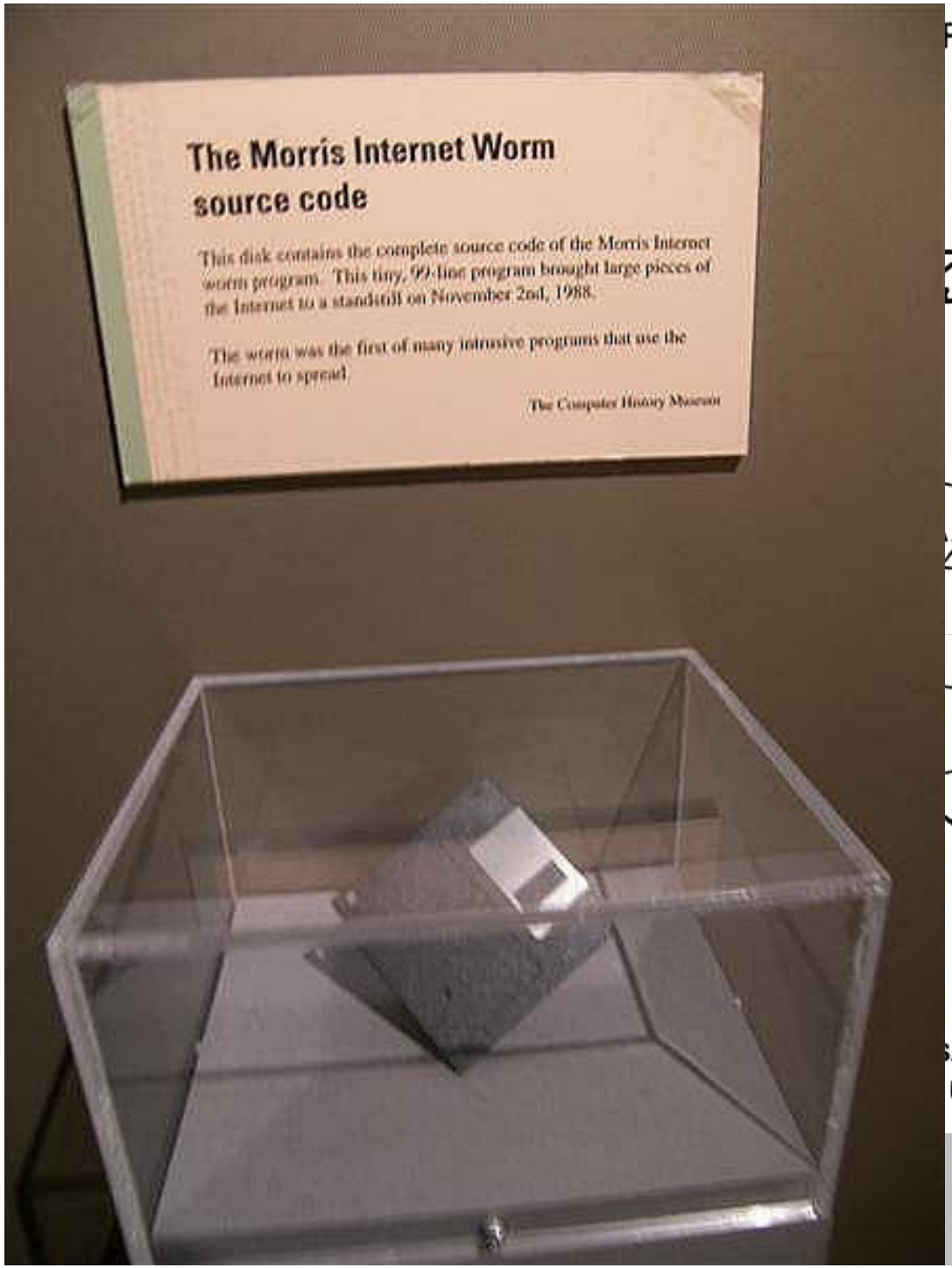
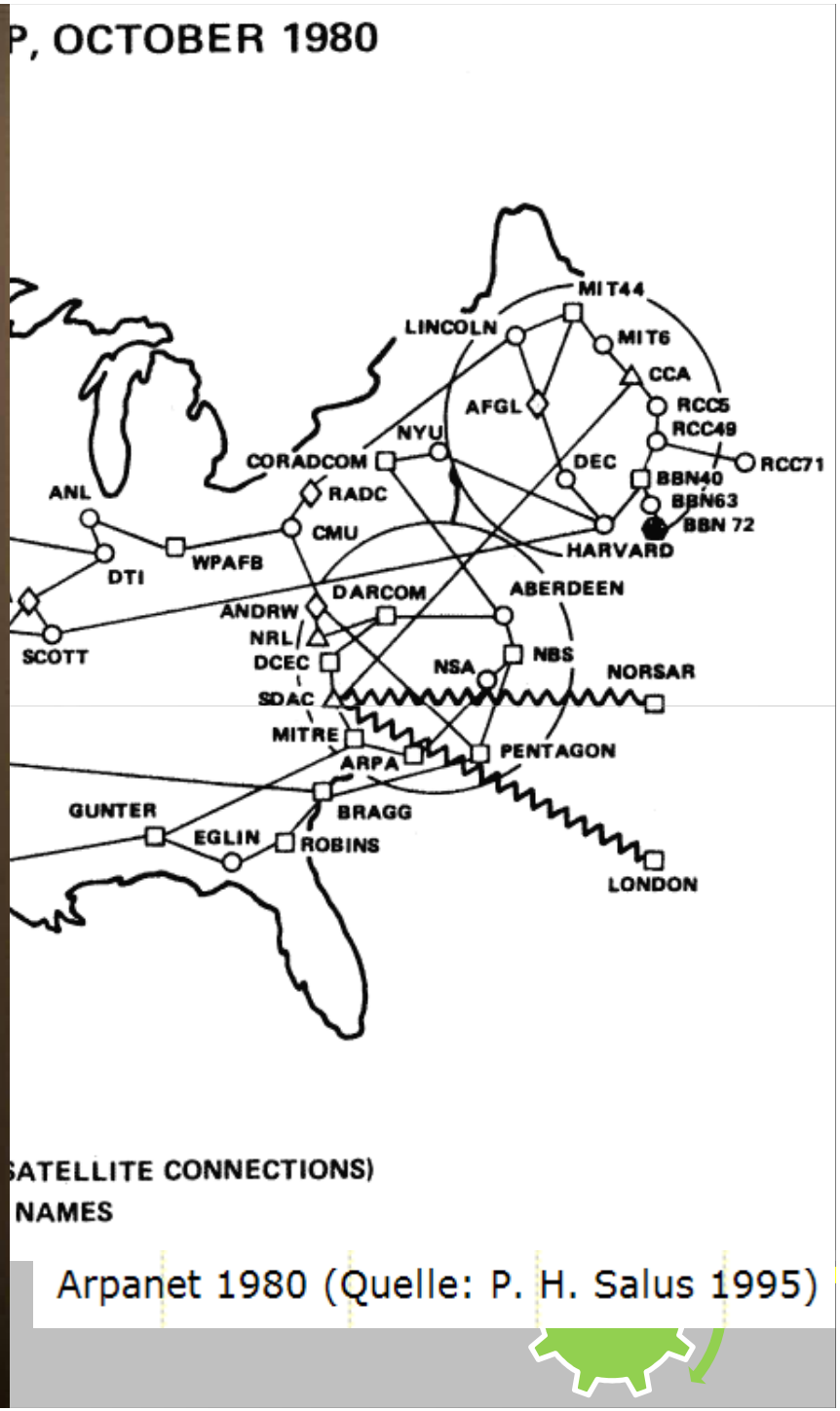
# CERT
# Computer Emergency Response Teams
# Kategorisierung

Dr. Otto HELLWIG






Arpanet 1980 (Quelle: P. H. Salus 1995)

# CERT Entstehung

1988 — CERT CC

1990 — FIRST

1998 — RFC 2350

1998 — Siemens CERT

2002 — CIRCA

2003 — ACOnet-CERT

2003 — US-CERT

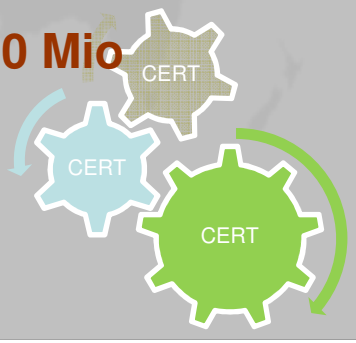
2008 — CERT.AT

1990 — 3 Mio

2000 — 360 Mio

2010 — 2.000 Mio

Internet User



# RFC 2350

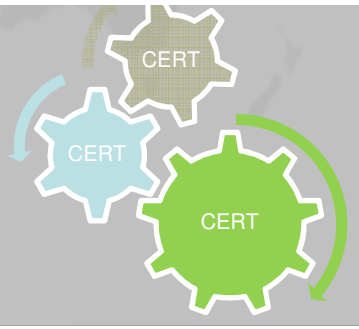
## Expectations for Computer Security Incident Response

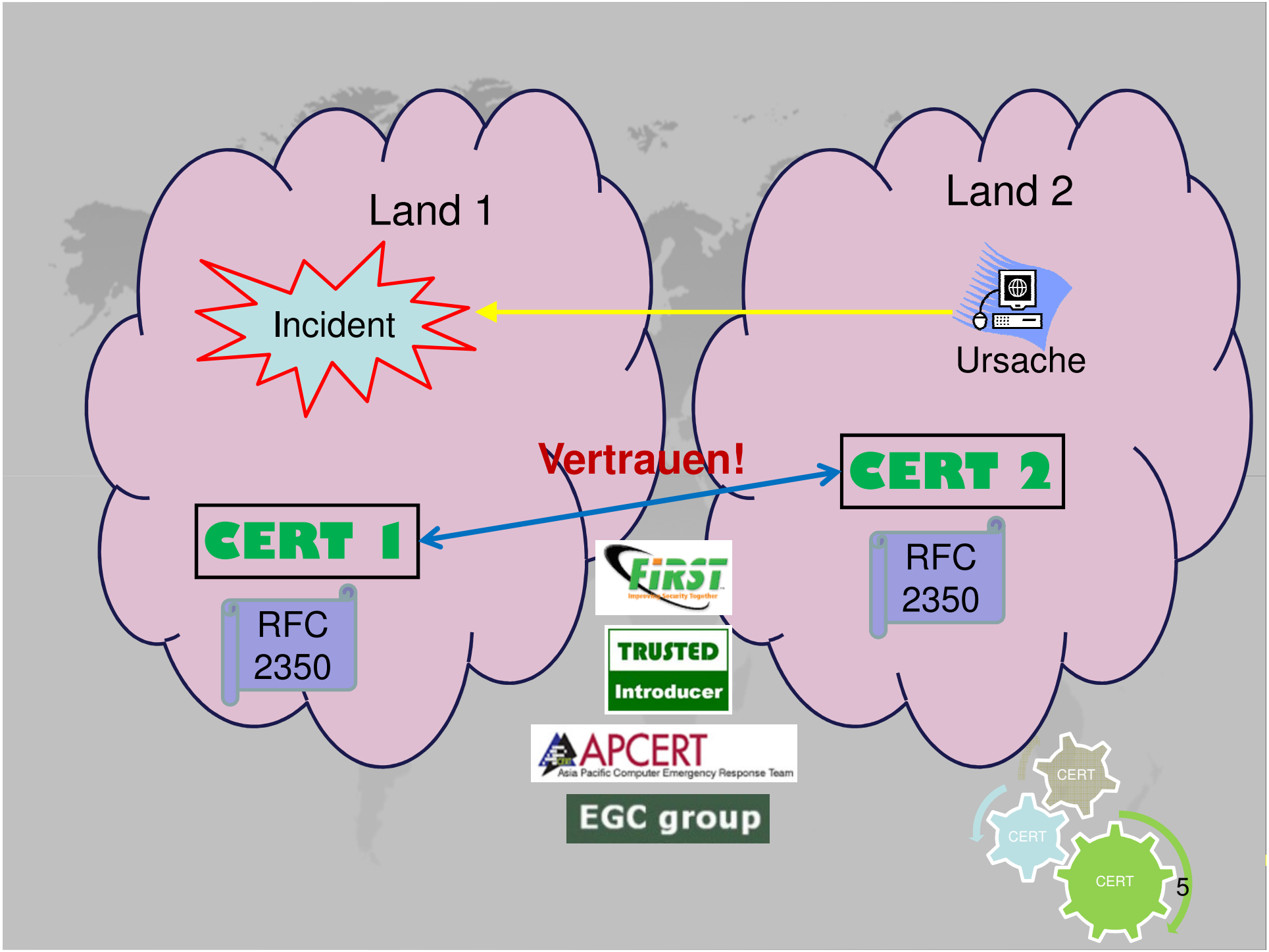
Constituency:

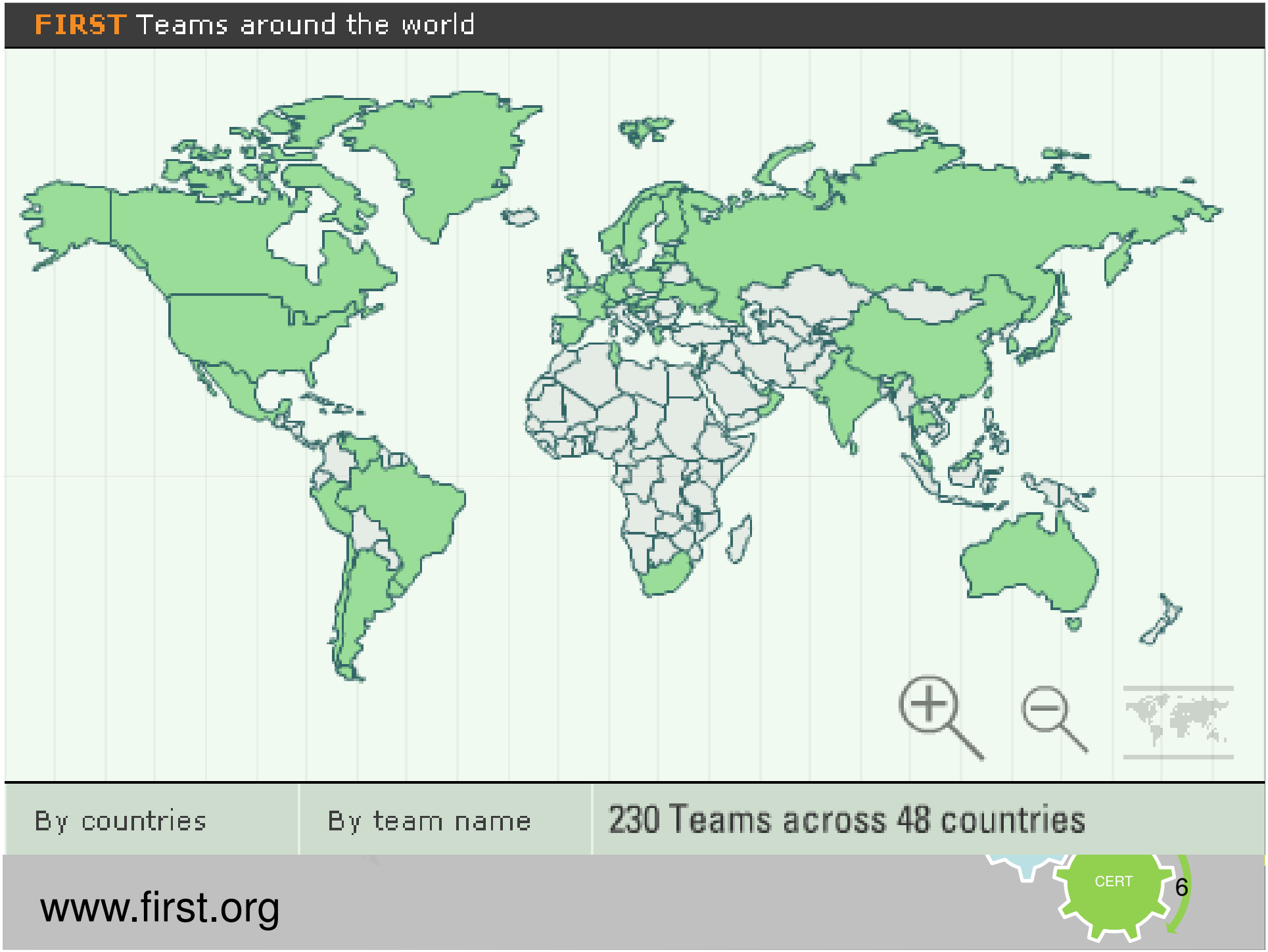
Implicit in the purpose of a Computer Security Incident Response Team is the existence of a constituency. This is the group of users, sites, networks or organizations served by the team. The team must be recognized by its constituency in order to be effective.

Security Incident:

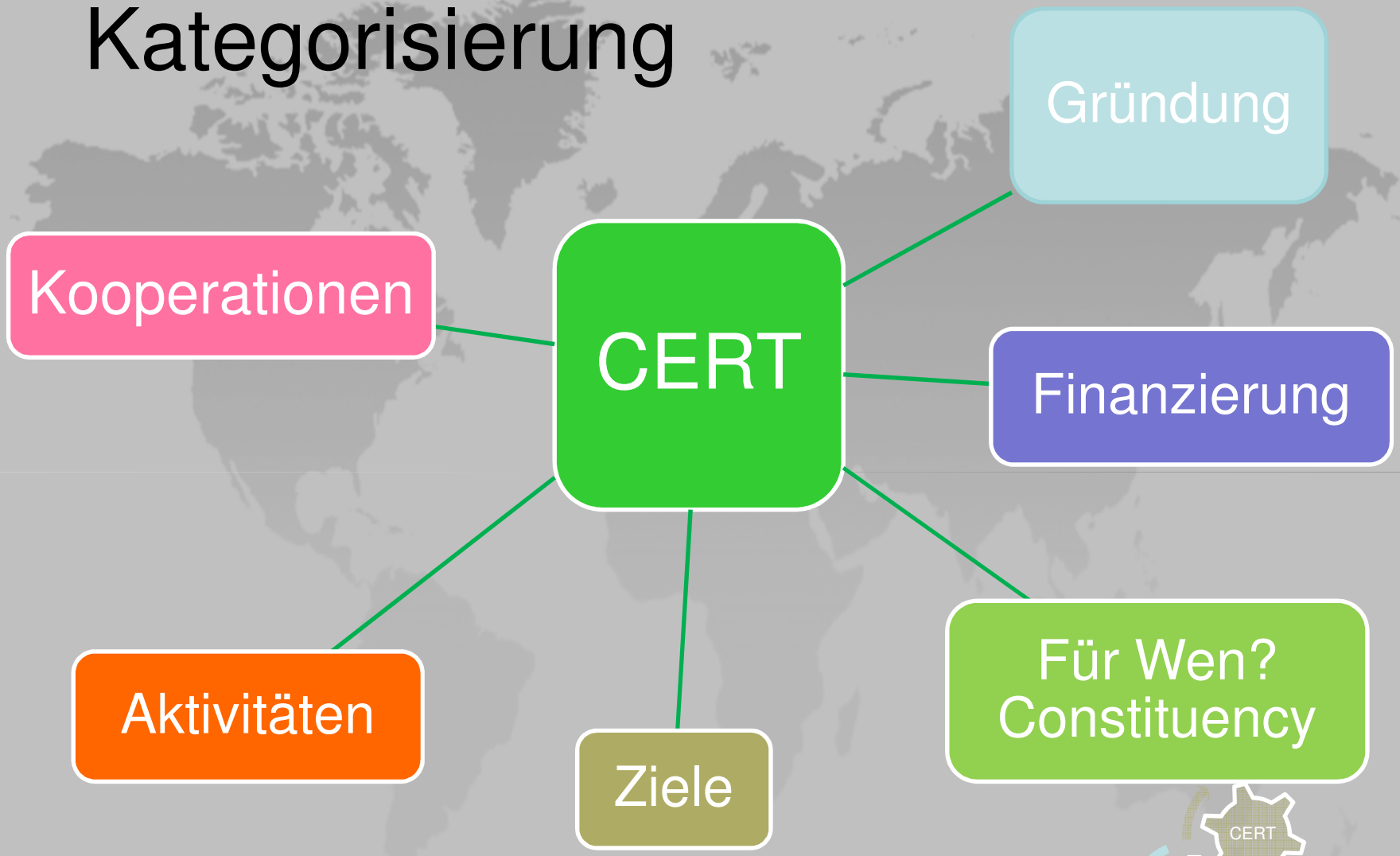
For the purpose of this document, this term is a synonym of Computer Security Incident: any adverse event which compromises some aspect of computer or network security.




Land 1
Land 2
Incident
Ursache
Vertrauen!
CERT 1
CERT 2
RFC 2350
RFC 2350
FIRST
TRUSTED Introducer
APCERT
Asia Pacific Computer Emergency Response Team
EGC group
CERT
CERT
CERT


FIRST Teams around the world
By countries
By team name
230 Teams across 48 countries
www.first.org
CERT
6

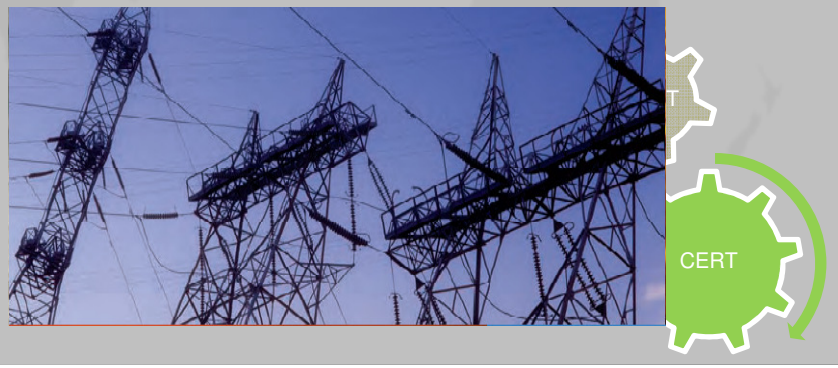
# Kategorisierung



# CERT Kategorien

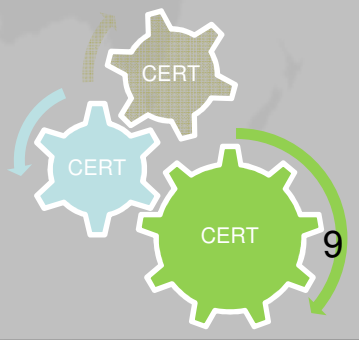
- Firmen-CERT
  - Firma
  - Dienstleistung
  - Produkt
- Government-CERT
- National

- Kritische Infrastrukturen



# Internationale Bestrebungen

- ITU: 2008, Resolution 58
  „Encourage the creation of national computer incident response teams, particularly for developing countries“
- G8
  Deklaration über Cyberkriminalität 2009
- EU
  Digitale Agenda
- ENISA:
  Anforderungen an GovCerts
  Information Sharing



# Conclusio - Ausblick

- Druck zur Schaffung und Nutzung von CERTs
- Verstärkte Kooperationen
  mit Strafverfolgung, mit ISP
  Themenbezogen mit anderen CERTs
- Internationale, übergreifende CERTs
  z.B. DNS CERT
  EU-CERT?
- CERTs und kritische Infrastrukturen
  cf. Stuxnet