CERT® Coordination Center

Building CSIRT Capabilities and the State of the Practice

Georgia Killcrece
CSIRT Development Team
CERT® Training and Education Center

August 7, 2003

CERT® Centers
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

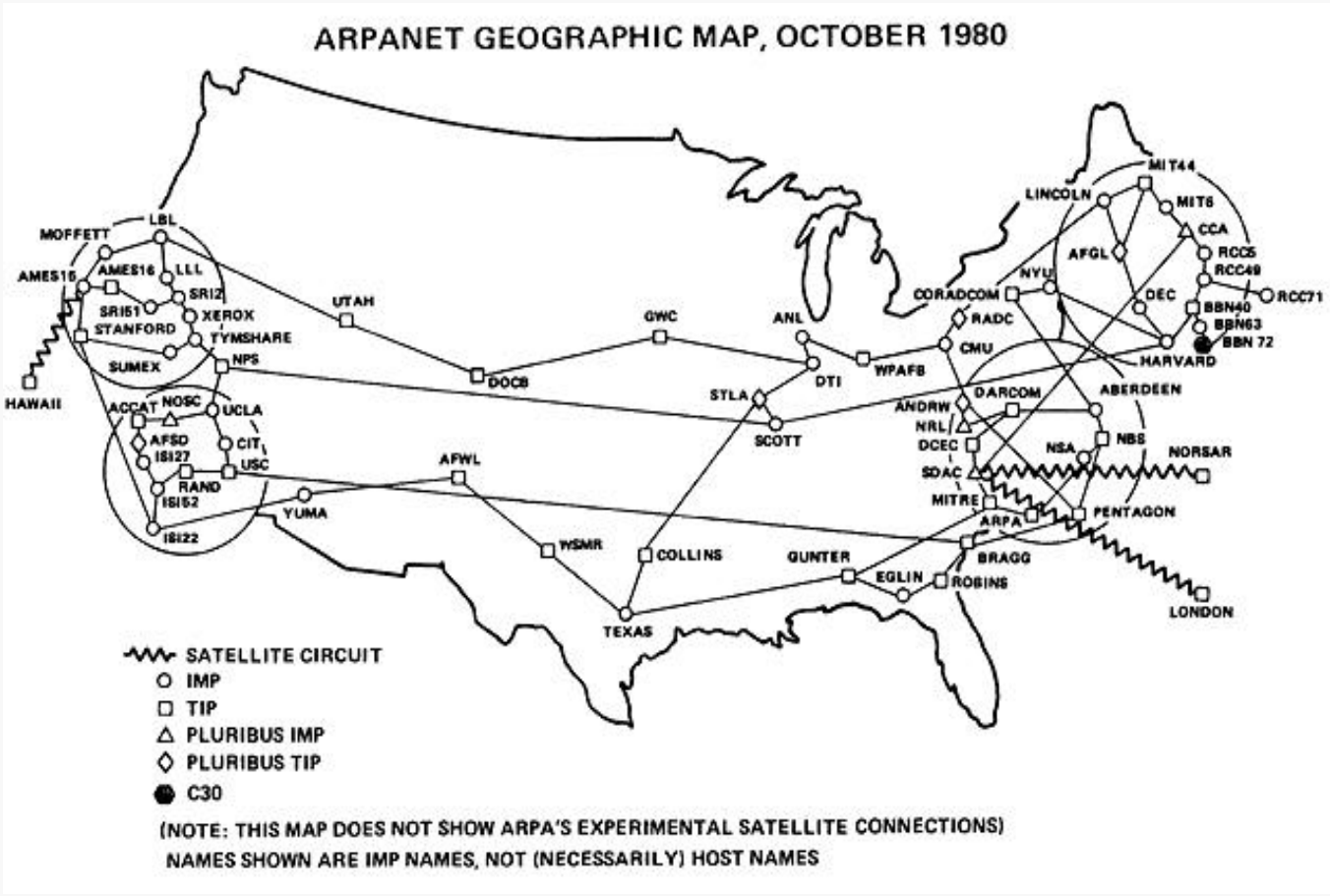
Sponsored by the U.S. Department of Defense

CERT® Coordination Center

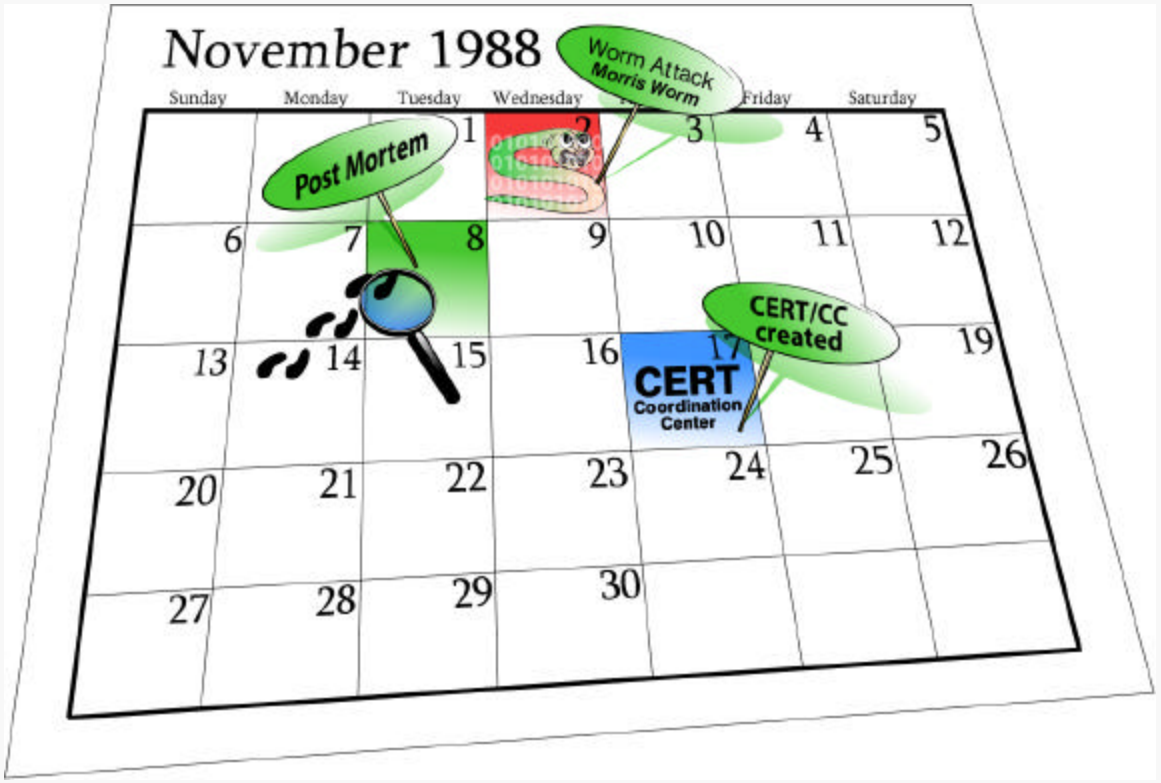
What is a CSIRT?

An organization or team within a defined constituency that provides services and support for preventing and responding to computer security incidents.

The Old "Net"



Early History*



***Timeframe: 1988. Approximate number of hosts: 60,000K**

CERT® Coordination Center

Initial Formation of Teams

FIRST Founding Members*

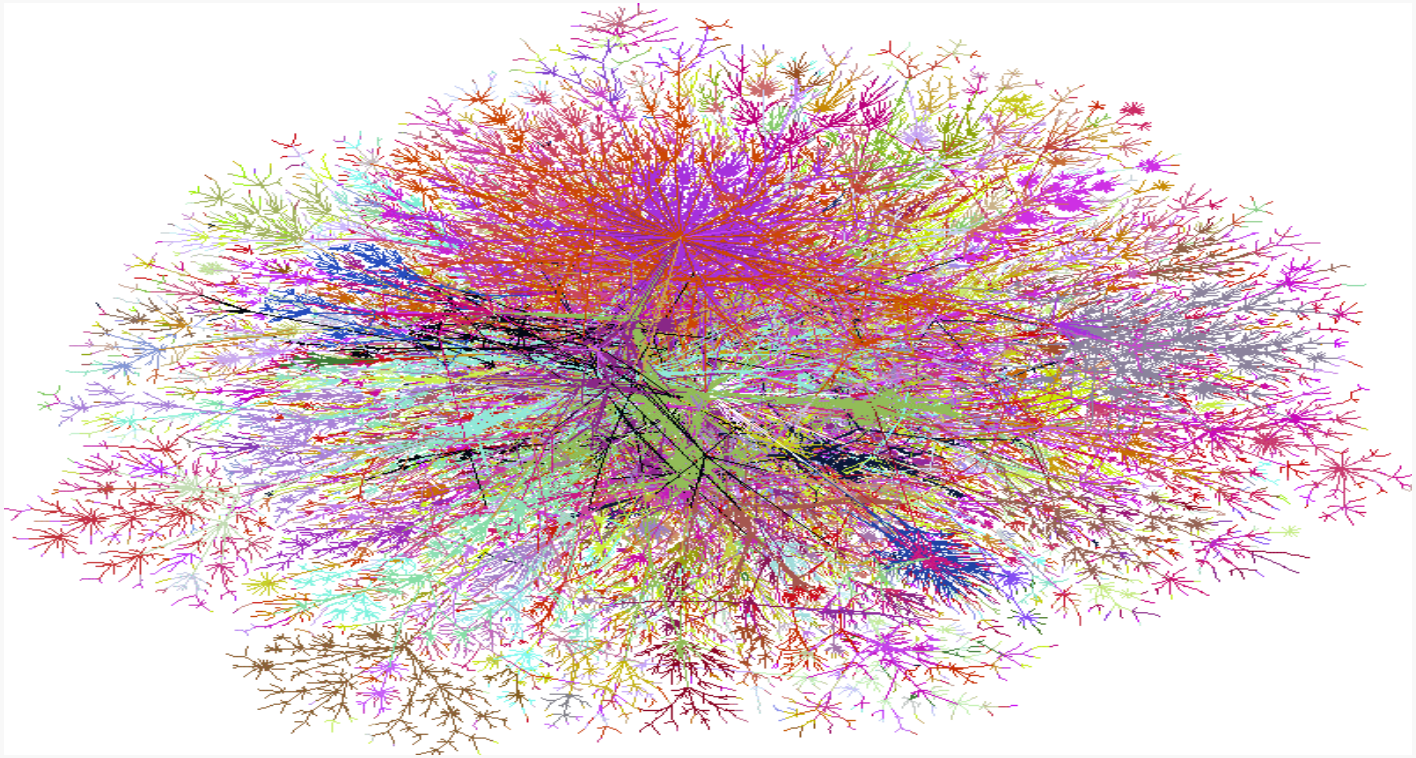
- **Air Force Computer Emergency Response Team (AFCERT)**
- **CERT Coordination Center**
- **Defense Communication Agency/Defense Data Network**
- **Department of Army Response Team**
- **Computer Incident Advisory Capability (CIAC)**
- **Goddard Space Flight Center**
- **NASA Ames Research Center**
- **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**

***Timeframe: 1990. Number of DNS advertised hosts: 340K**

CERT Coordination Center 15 Years of Service 1988 - 2003

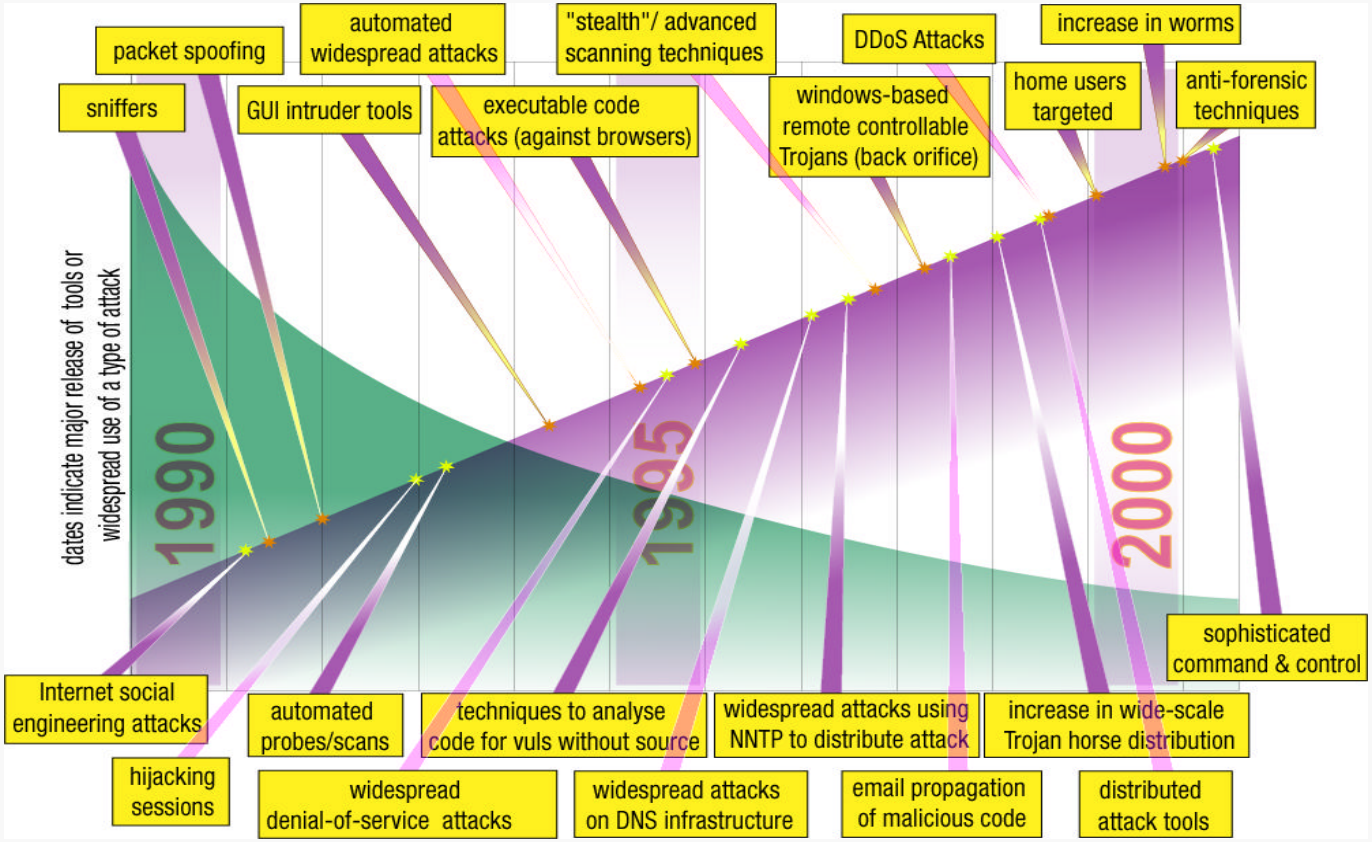
CERT® Coordination Center

The New “Net”

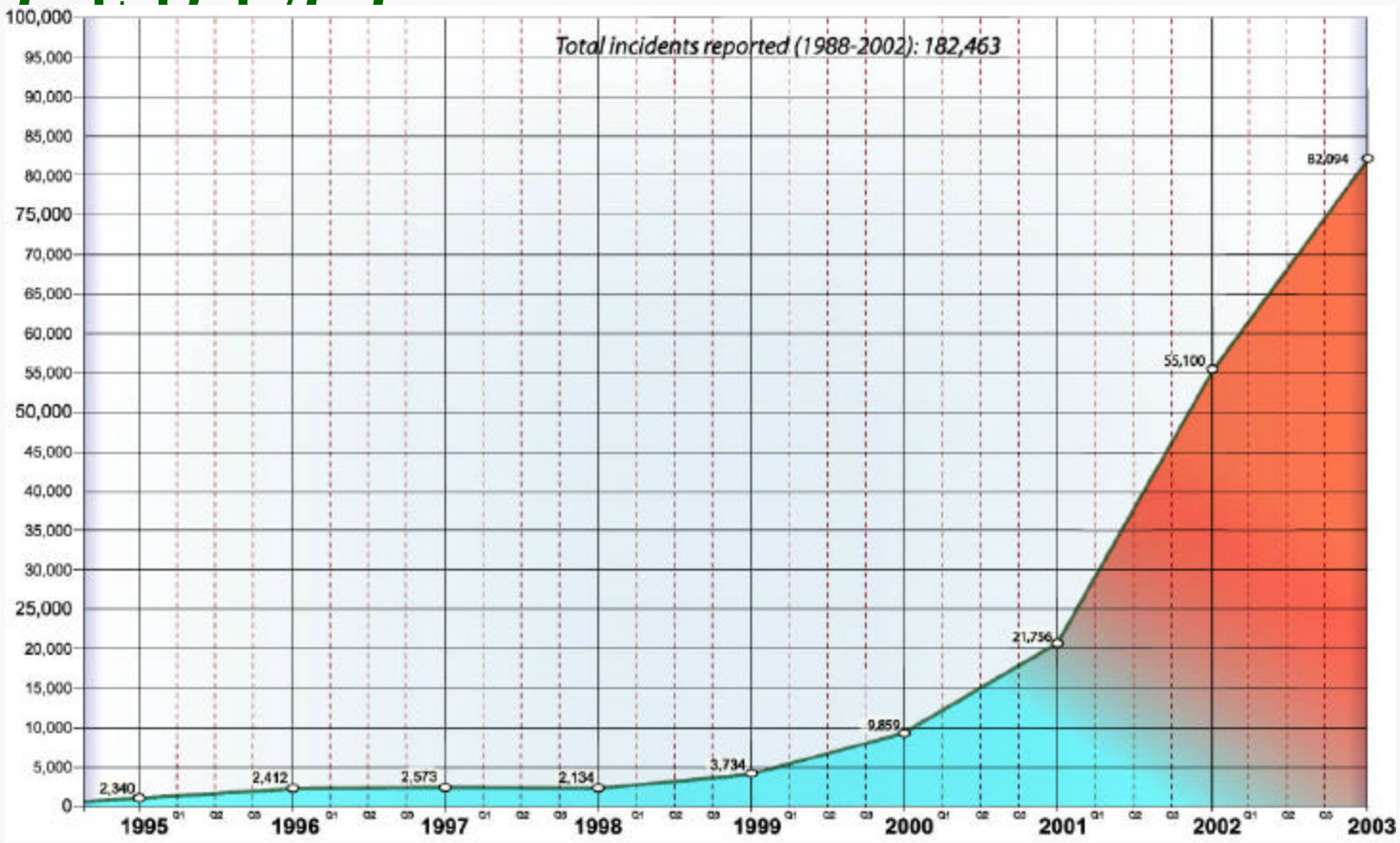


Source: http://cm.bell-labs.com/who/ches/map/gallery/index.html

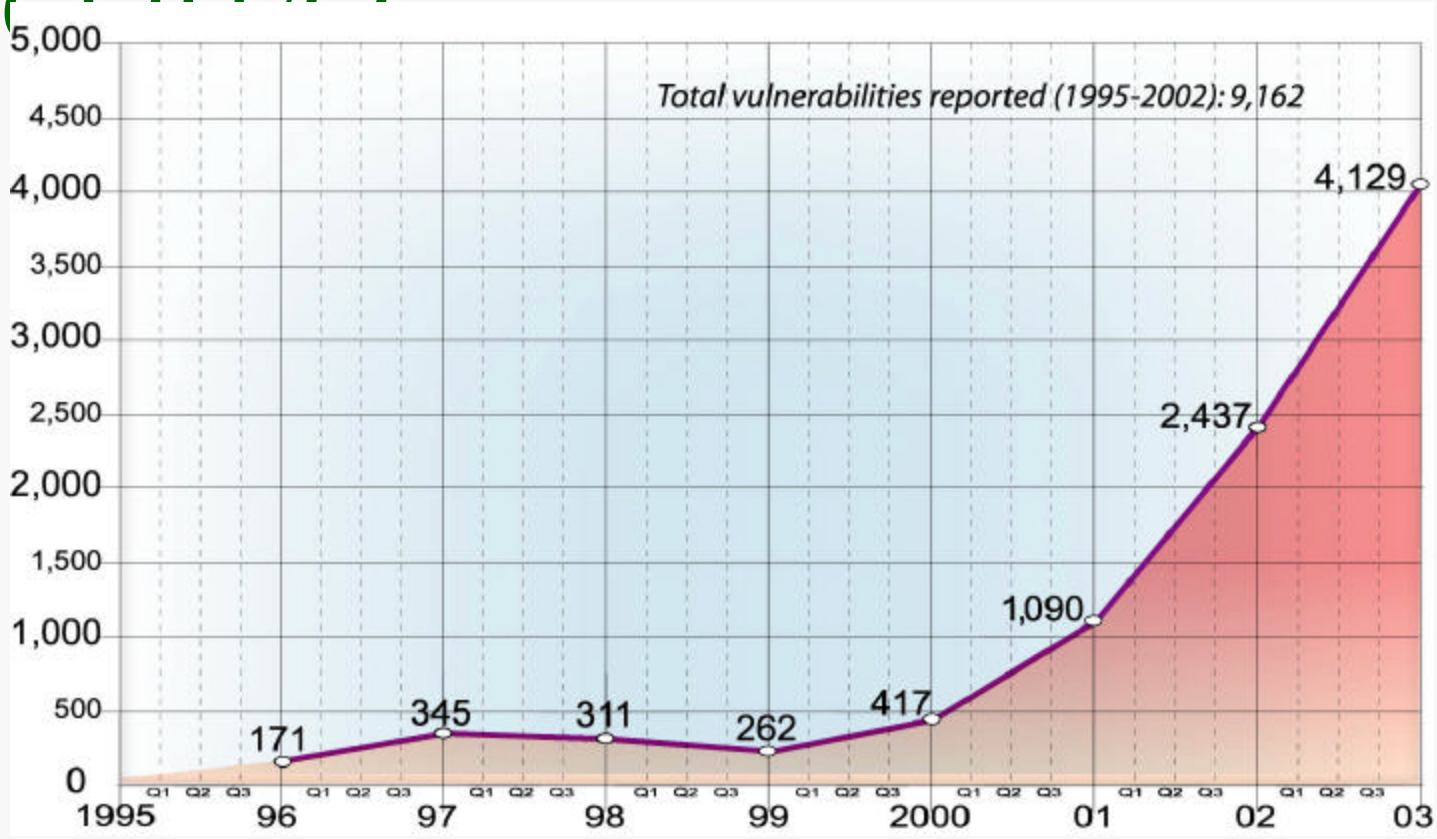
Attack Sophistication vs. Required Intruder Knowledge



Growth in Number of Incidents Reported to CERT/CC



Growth in Number of Vulnerabilities Reported to CERT/CC



CERT® Coordination Center

CERT Coordination Center 15 Years of Service 1988 - 2003

Impact on CSIRTs

Today's dynamic environment means less time for CSIRTs to react.

Therefore, teams require

- **a method for quick notification**
- **established and understood policies and procedures**
- **automation of incident handling tasks**
- **methods to collaborate and share information with others**
- **easy and efficient way to sort through all incoming information**

CERT® Coordination Center

Current Situation

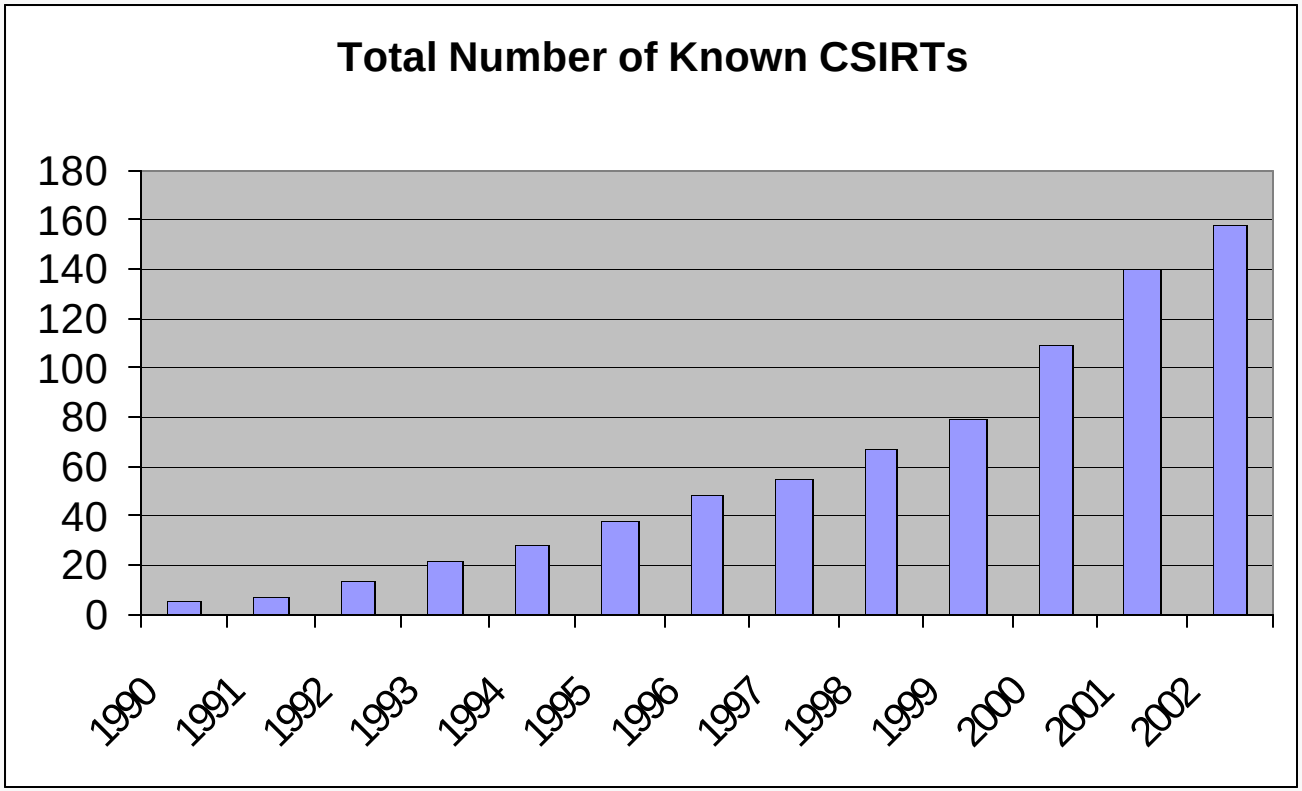
Many organizations do not have a formalized incident response capability.

There is a shortage of effective CSIRTs and trained staff to respond to current and emerging computer security threats.

A growing number of organizations are

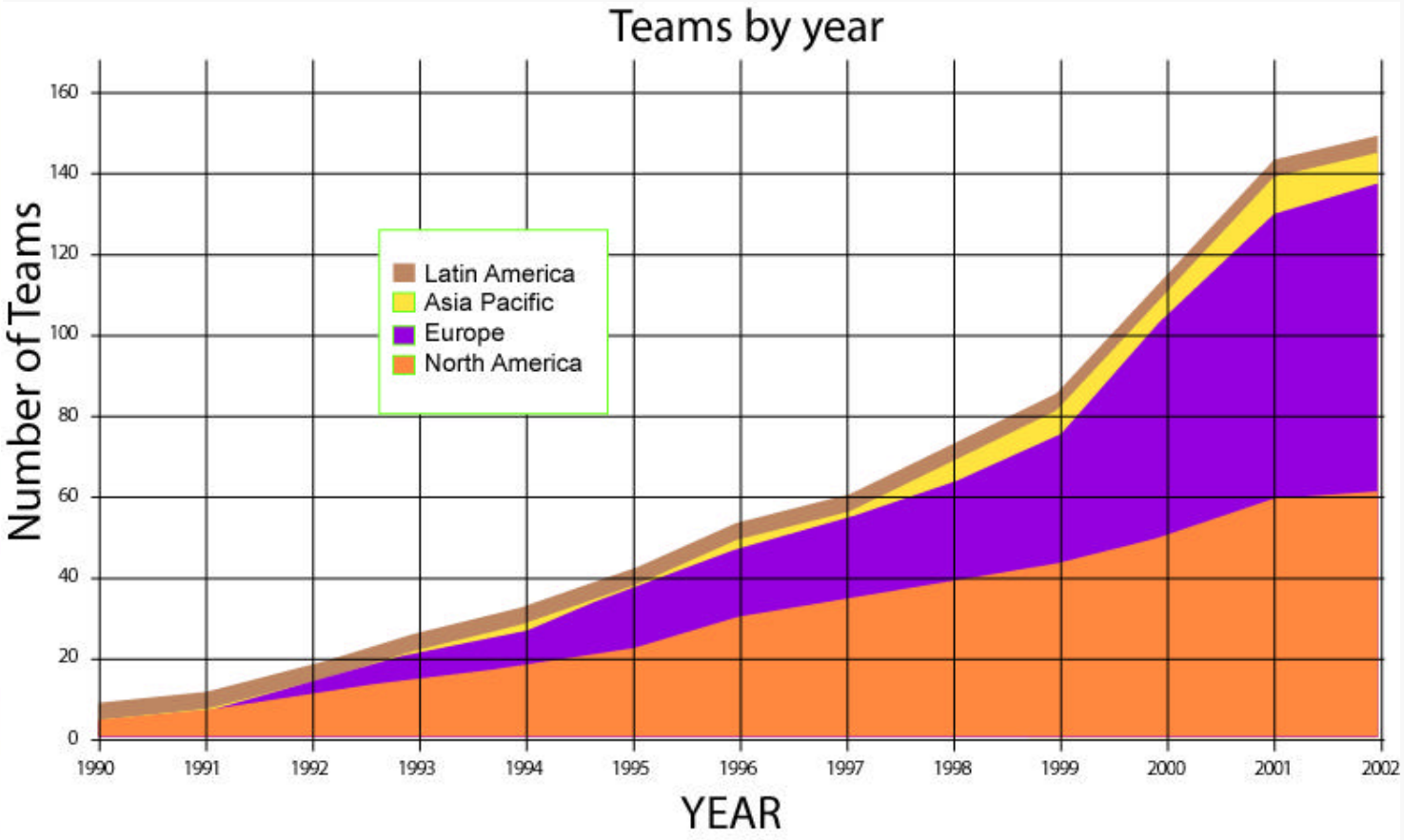
- **being mandated or required by laws/regulations to have an incident response plan in place**
- **proactively seeking to implement a CSIRT as a part of their information security program.**

Number of Known Teams*



***Timeframe: 2002. Number of DNS advertised hosts: 171.6 billion.**
Note: These are teams we know about, there are many more teams that exist.

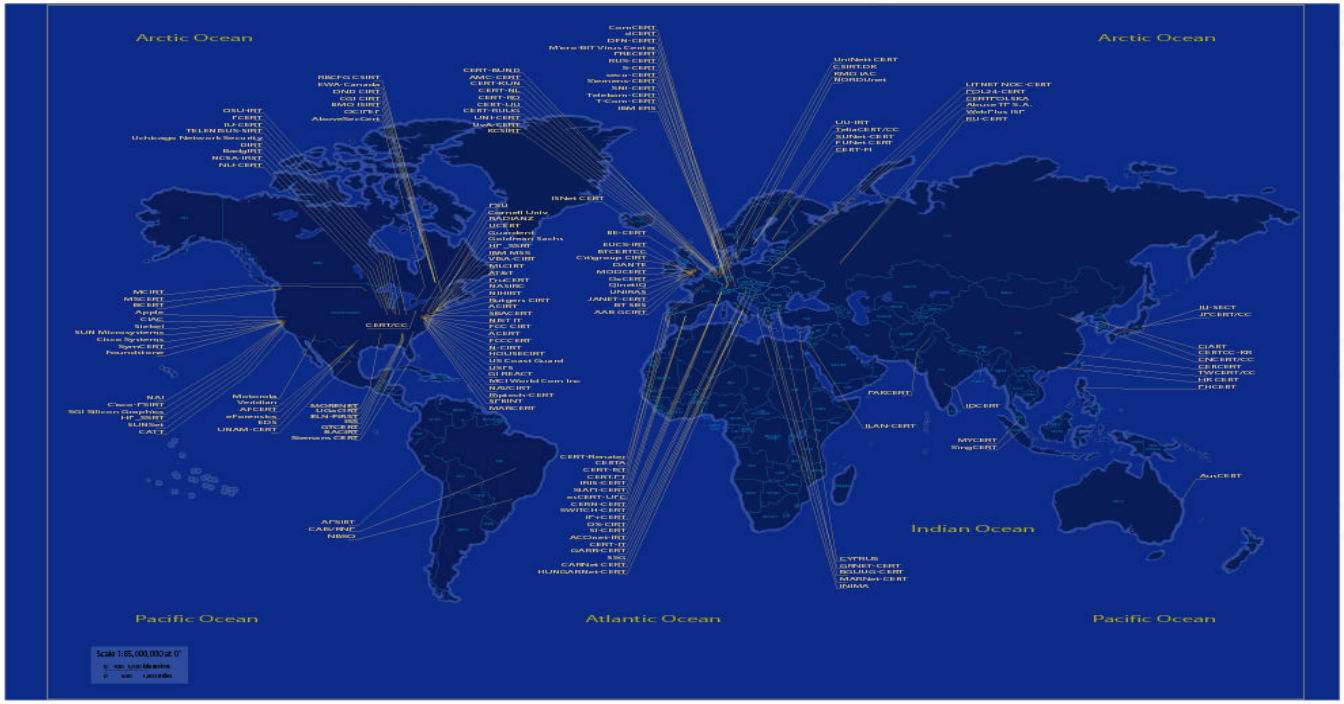
Growth in CSIRTs by Region



Geographic Dispersion

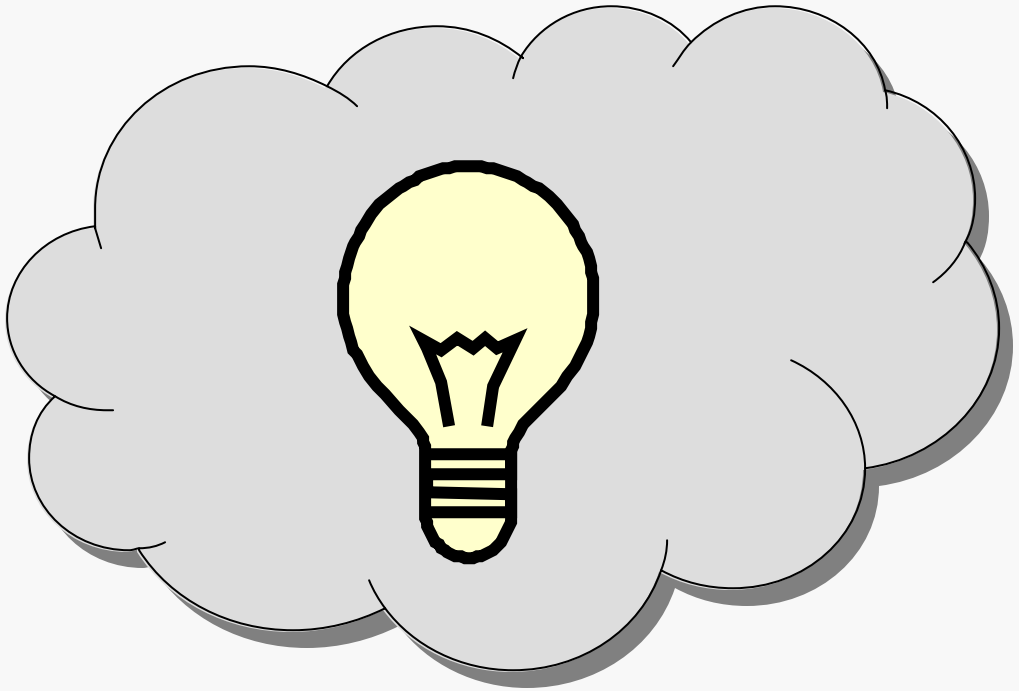
Incident Response Teams Around the World

International cooperation speeds response to Internet



CERT® Coordination Center

Where Do You Start?



Stages of CSIRT Development

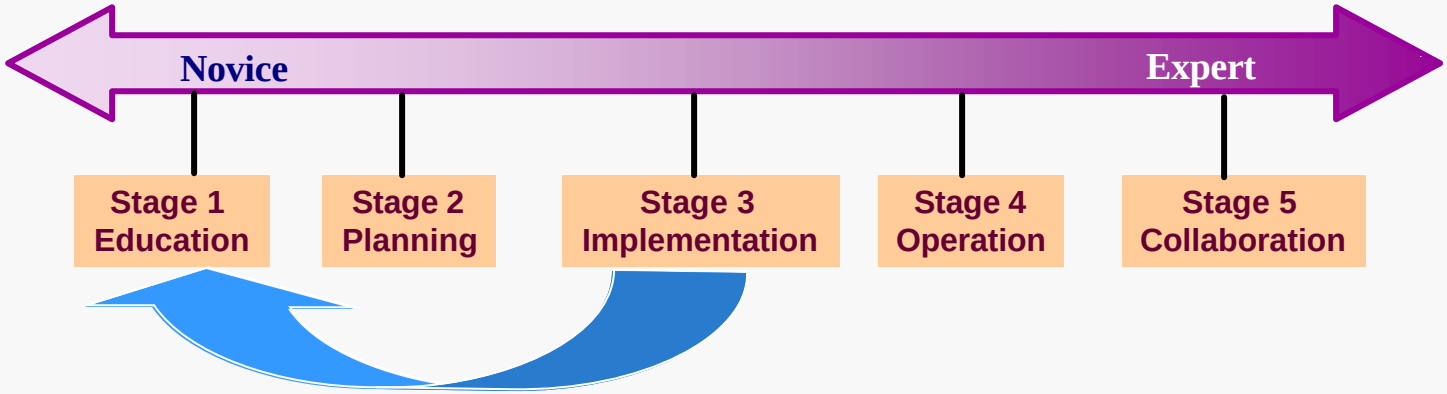
Stage 1 **Educating the organization**

Stage 2 **Planning effort**

Stage 3 **Initial implementation**

Stage 4 **Operational phase**

Stage 5 **Peer collaboration**



CERT® Coordination Center

CSIRT Related Projects

A sample of current CSIRT projects include

- **State of the Practice of CSIRTs**
- **IETF Incident Handling Working Group (INCH WG) and Intrusion Detection Working Group (IDWG)**
- **Automated Incident Reporting (AirCERT)**
- **Incident Detection, Analysis, and Response (IDAR) Project**
- **Clearing House for Incident Handling Tools (CHIHT)**
- **Common Advisory Interchange Format (CAIF)**
- **Best Practices Documents (RFC 3227, 2350)**

CERT Coordination Center 15 Years of Service 1988 - 2003

CERT® Coordination Center

Current CSIRT Discussion Topics

Legal issues and impacts

Automation and standardization of CSIRT tools

Data sharing and collaboration

Certification for incident handlers and teams

Regionalization efforts

CERT® Coordination Center

AirCERT

Components include:

- sensor(s) and site database(s) at a participating organization
  - a set of defined attack signatures
  - a central database at the CERT/CC
  - a mechanism for the transmission of data
    between sensors and the site database
    between the site and central databases
- communication protocols
  - sensor-to-site database
  - site database-to-central database

CERT Coordination Center 15 Years of Service 1988 - 2003

CERT® Coordination Center

Benefits of AirCERT

For participants:

- collect information on activity within their organizations
- receive aggregated feedback from the CERT/CC
- use defined methods of collecting and sharing incident information*

For the Internet community:

- receive and collate data in near real-time
- provide timely information about attacks
- faster release of new attack signatures
- provide structured and statistically significant data

*IETF, Intrusion Detection Message Exchange Requirements

CERT® Coordination Center

For More Information

CSIRT Development Team
CERT ® Training and Education Center
CERT® Centers
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213 USA
+1 (412) 268-7090

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

CERT Coordination Center 15 Years of Service 1988 - 2003