CERT

CERT/CC Overview & CSIRT Development Team Activities

Georgia Killcrece
CSIRT Development Team
CERT® Program
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
October 2006

Software Engineering Institute

Topics

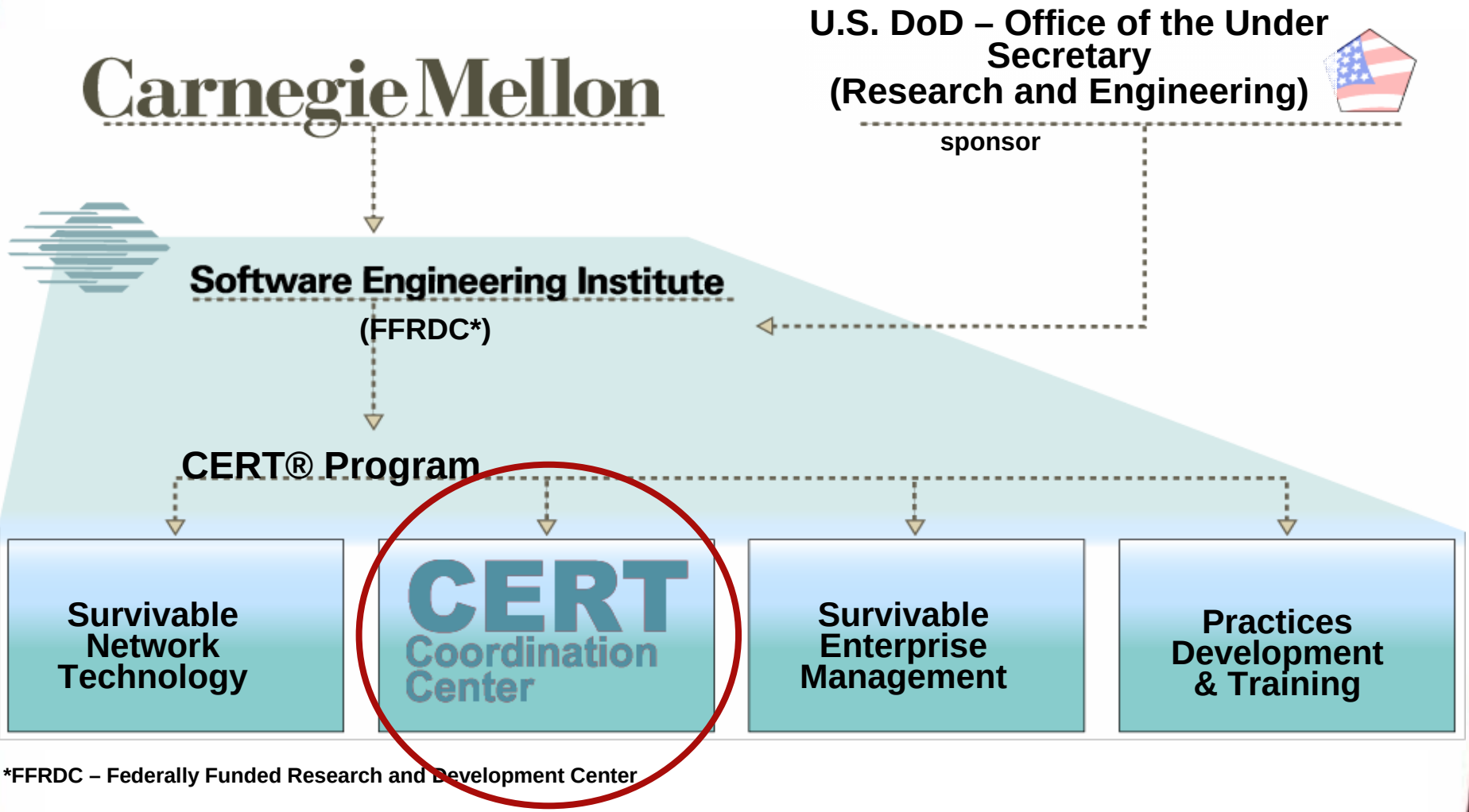
CERT/CC – background history and current work

Practices, Development, and Training – the Educational and Training activities we're undertaking

CSIRT Development Team – an overview of the activities related to developing CSIRTs and incident management best practices

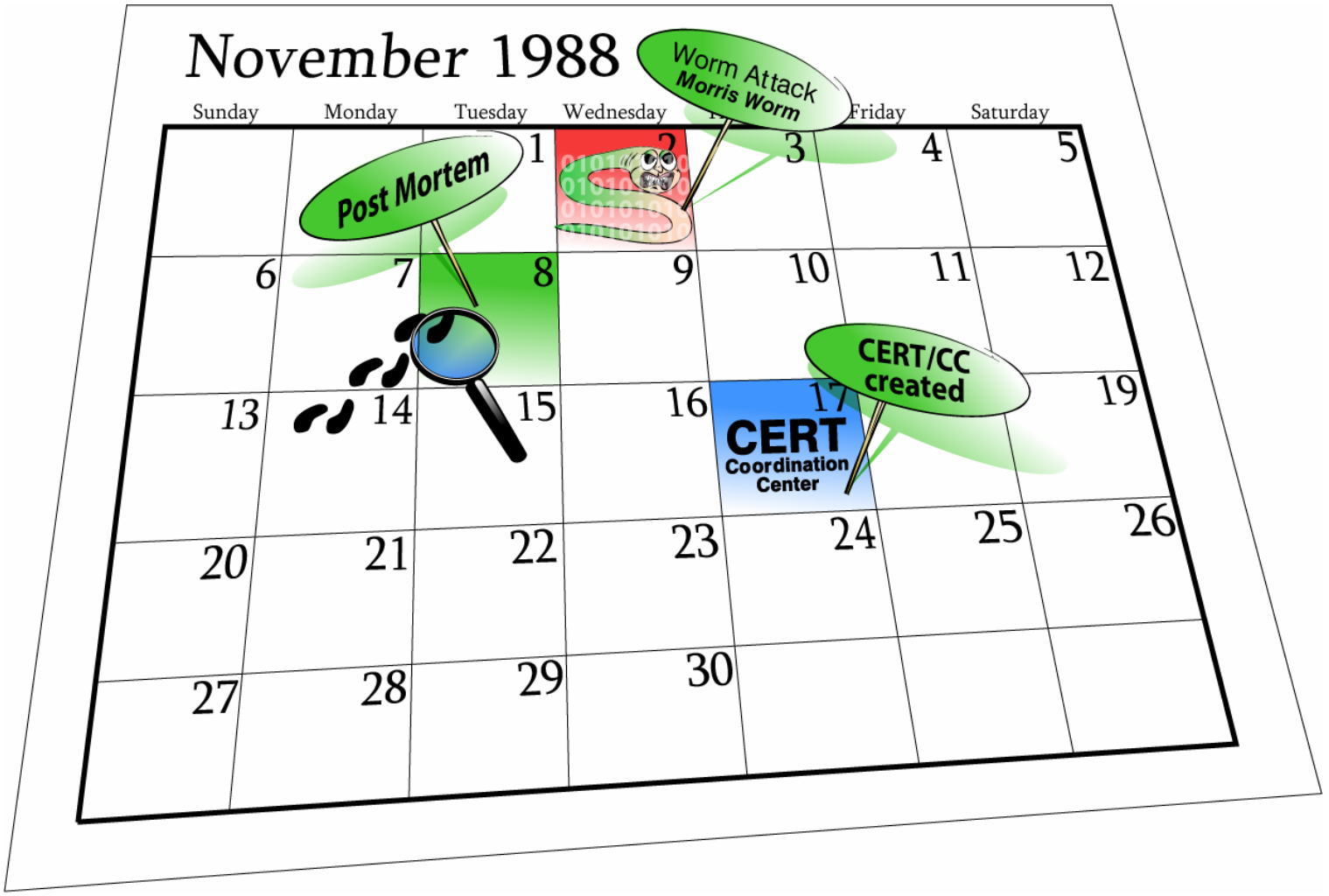
CERT/CC

Organizational Hierarchy



*FFRDC – Federally Funded Research and Development Center

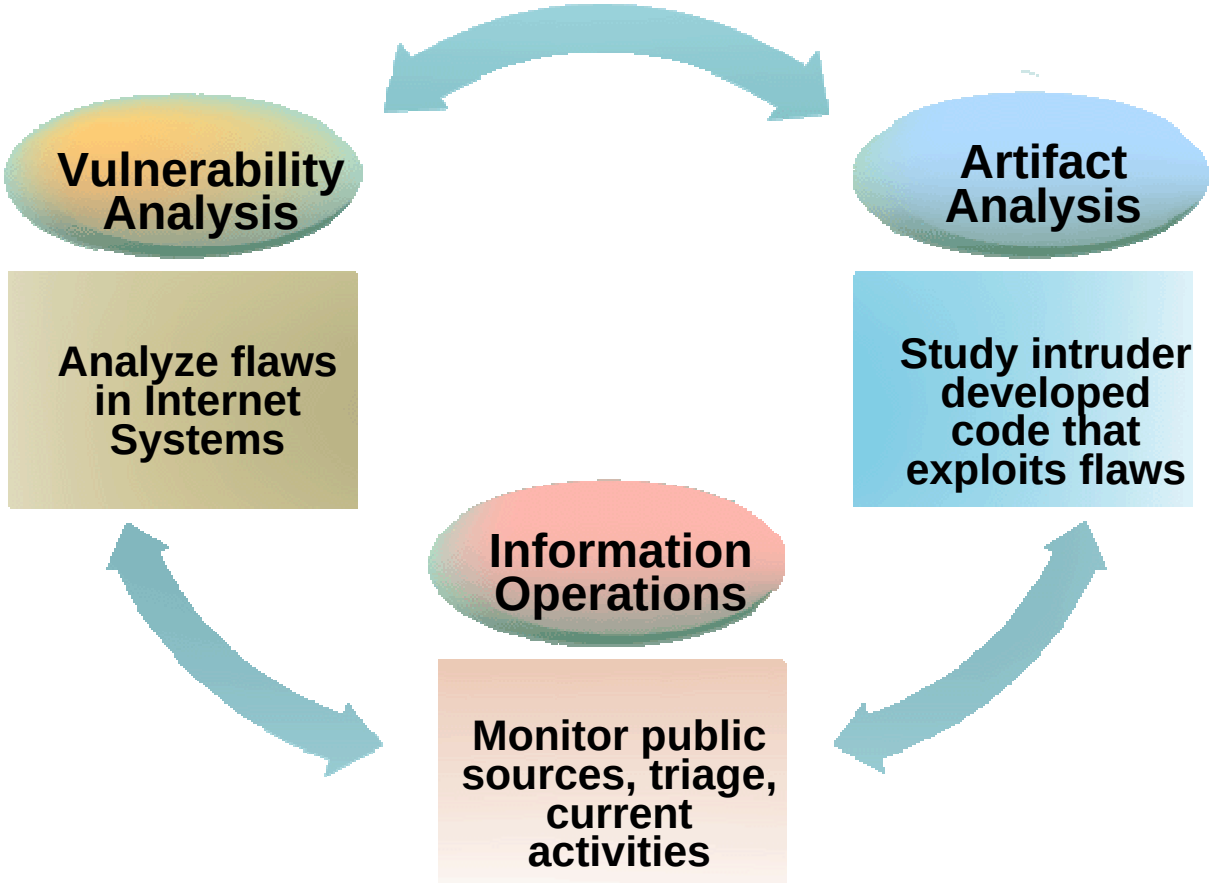
CERT/CC Beginnings



CERT/CC Mission

- Provide a reliable, trusted, 24-hour, single point of contact for emergencies.
- Facilitate communication among experts working to solve security problems.
- Serve as a central point for identifying and correcting vulnerabilities in computer systems.
- Maintain close ties with research activities and conduct research to improve the security of existing systems.
- Initiate proactive measures to increase awareness and understanding of information security and computer security issues throughout the community of network users and service providers.

CERT/CC Activities



CERT/CC Outreach and Collaboration

Resident Affiliates

Foster collaborative efforts and information sharing

Regularly attend and present at conferences, including

- FIRST www.first.org
- IETF www.ietf.org
- InfraGard www.infragard.net
- NANOG www.nanog.org
- AUSCERT www.auscert.org.au
- GOVCERT www.govcert.nl
- NSTAC NSIE www.ncs.gov/NSTAC/nstac.html
- USENIX www.usenix.org
  - LISA
  - Security Symposium
  - Technical Conference

Example: CERT/CC and US-CERT

US-CERT was established in September 2003 as a public-private partnership charged with improving computer security preparedness and response to cyber attacks in the United States.

- As an institution, US-CERT is responsible for
- analyzing and reducing cyber threats and vulnerabilities
- disseminating cyber threat warning information
- coordinating incident response activities

US-CERT also provides a way for citizens, businesses, and other institutions to communicate and coordinate directly with the United States government about cyber security.

US-CERT is a partnership of

- the National Cyber Security Division (NCSD) of the Department of Homeland Security (DHS)
- the CERT Coordination Center

CERT/CC and US-CERT: Products and Resources

Technical Cyber Security Alerts

Cyber Security Alerts (Non-technical)

Vulnerability Notes

Cyber Security Bulletins

Cyber Security Tips

Current Activity

New Threats and Vulnerabilities Bring New Risks

Threats

- Disgruntled Employees
- Hackers for hire
- Organized Crime
- Competitors
- Cyber Vandals
- Governments

Vulnerabilities

- OS
- Network
- Applications
- Databases
- PCs, PDA, Phones
- Middleware
- E-x Communities (e-government, e-commerce, etc)

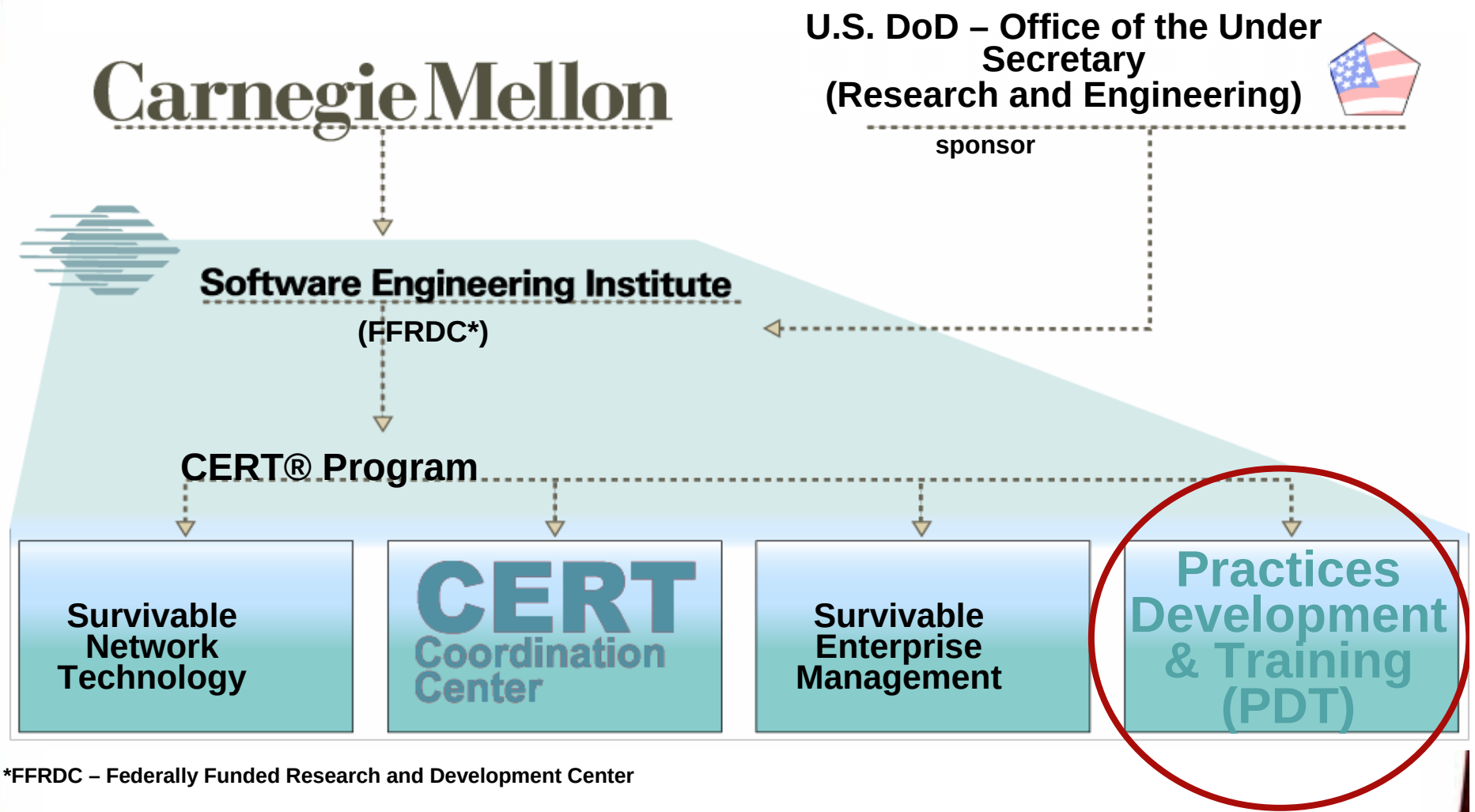
Risks

- Disclosure of Customer Records
- Sabotage of Operations/Service
- Extortion
- Theft of Trade Secrets
- EFT Fraud
- Loss of Client Confidence
- Legal Liability

Impact: "*Last year was the first year that proceeds from cybercrime were greater than proceeds from the sale of illegal drugs, and that was, I believe, over $105 billion*." Valerie McNiven, a U.S. Treasury Department expert on cybercrime, interview with Reuters November 28, 2005.

Practices, Development, & Training

Organizational Hierarchy



*FFRDC – Federally Funded Research and Development Center

PDT Vision

An Internet community that is

- Aware
- Knowledgeable
- Trained
- Educated

in information science

CERT

Strategic Goals

Anytime, anywhere learning

Millions of users

Leading edge technical content

Knowledge in Depth for Defense in Depth

FY06 Key PDT Objectives

Create a knowledgebase of network forensics practices, methodologies, tools, and catalog for use by law enforcement, incident response teams, first responder IT staff, and system and network operators

Develop a proof of concept operational virtual forensics lab for strategic customers

Develop the Virtual Training Environment as a comprehensive IA capability for meeting DoD certification requirements

Pilot, refine and transition a methodology and set of metrics to assess computer security incident management capability for federal civilian agencies

Transition the SIA curriculum to academic institutions

PDT Impact Metrics – Q1-3 FY06

Publications	4
Courses offered / students	29 / 888
Conferences/workshops	2
VTE users	58,500
SIA curriculum users/countries	769/80
Licensees	7
Presentations/Keynotes	16
Awards	1
New technologies/technical products released	6

PDT Staff – Q1-3 FY06

Full Time Staff hired	7
Total full time staff	23
Visiting Scientists	14
Graduate Students	11
Staff on INI faculty	3

PDT Teams

Information Assurance Practices

Cyber Forensics

CSIRT Development

Training

Virtual Training Environment

Outreach and Education

Today's Challenges Impact CSIRTs

Less time to react

Need for

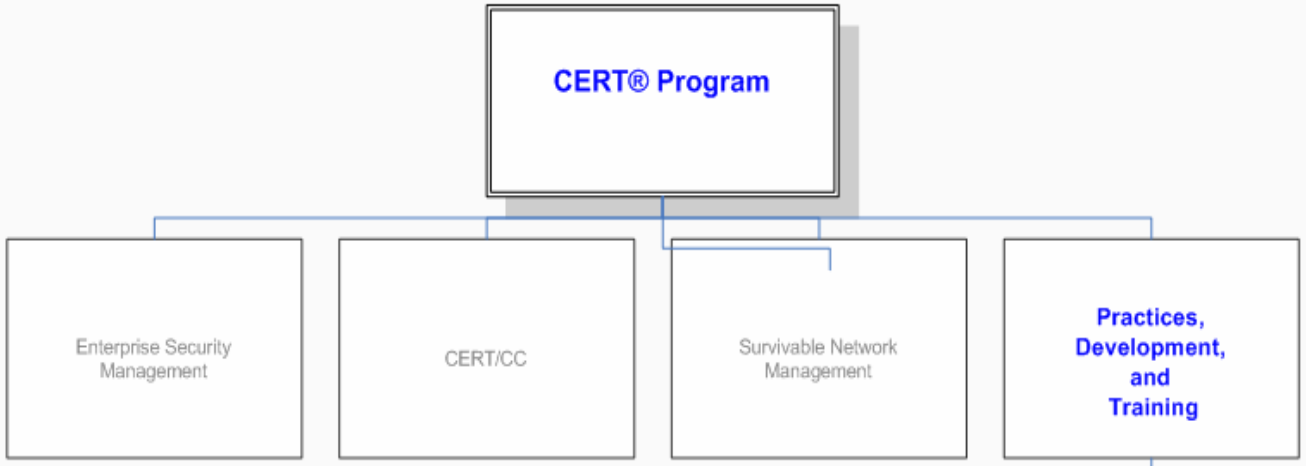
- quick notification
- automation of incident handling tasks
- easy and efficient means to sort and analyze information
- effective mechanisms to collaborate and share information

Requirement for

- well-defined policies and procedures
- streamlined business processes to effectively manage and respond to events and incidents
- personnel with the knowledge, skills, and abilities to perform the work

CSIRT Development Team

Organizational Hierarchy



CSIRT Development Team

Georgia Killcrece, Team Lead
Audrey Dorofee
Robin Ruefle
Mark Zajicek

Visiting Scientists: 9
Administrative Staff: 1

September 22, 2006

CERT

CSIRT Mission

Foster the growth of global incident management capabilities.

Assist national and international organizations in establishing effective CSIRTs.

Help existing CSIRTs improve their services and operation through training, mentoring, and collaboration.

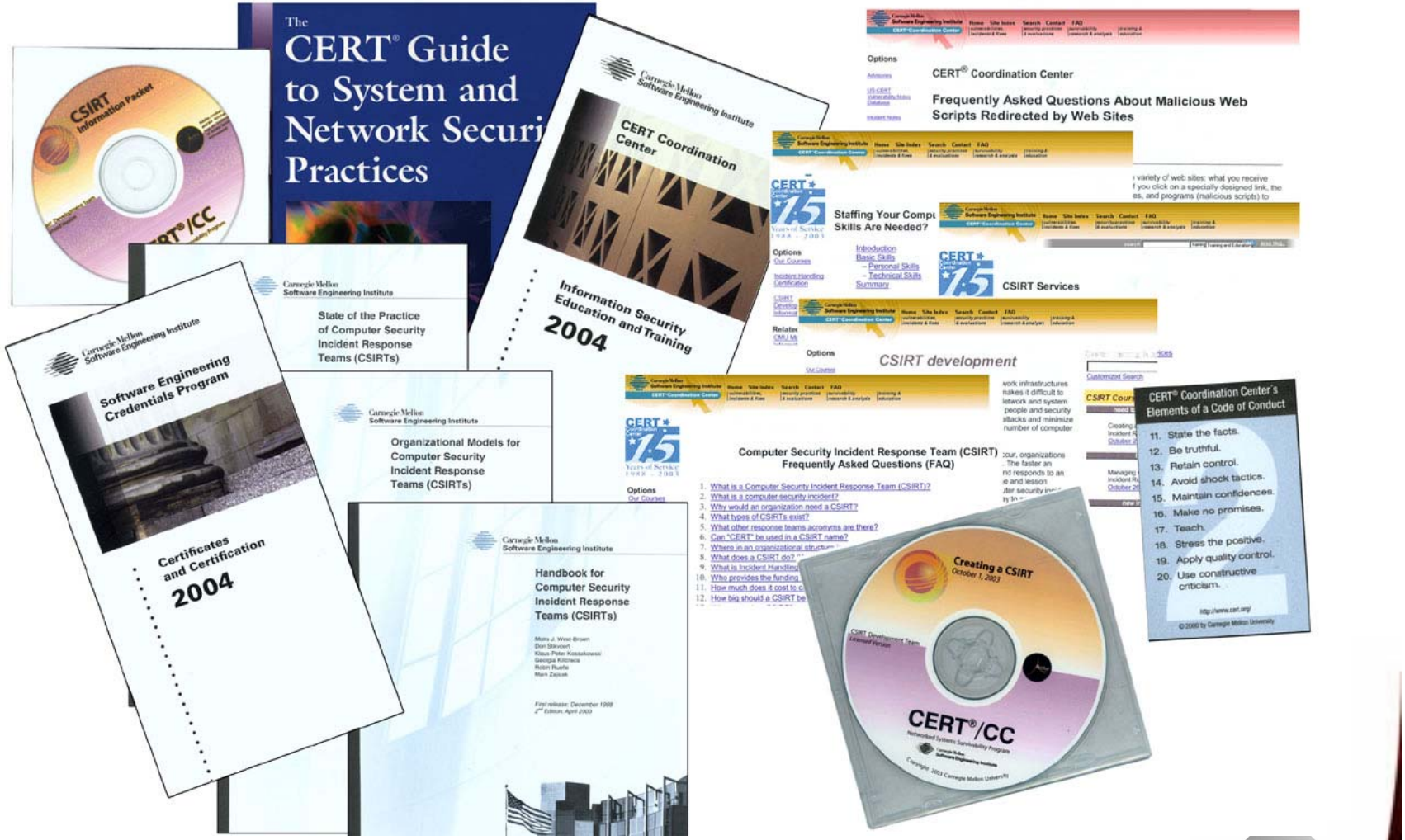
Create

Amplify

Transition

CERT

Products and Publications



CERT

CSIRT Development Team Activities -1

Research into the current incident management environment

- synthesize existing information and best practices into guides, standards, and methodologies for performing incident handling processes and functions
- identify methods for measuring the effectiveness of CSIRT capabilities (teams and personnel)

Initiatives with other stakeholders to

- develop strategies to plan and implement CSIRTs
- create best practices for operating CSIRTs
- implement CSIRT policies and standard operating procedures

Creating products that promote CSIRT development by

- collaborating with other teams and experts to build a CSIRT Body of Knowledge

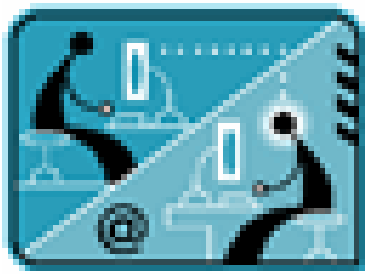
Strategic Initiatives

Working with Department of Defense (DoD)

- DoD 8530 Computer Network Defense (CND) Service Provider evaluation metrics
- DoD 8570 Information Assurance Training, Certification, and Workforce Management (functional requirements for CND Service Providers)

Federal Government (US-CERT)

- Adapting DoD metrics for use within US Federal civilian agencies



CSIRT Development Team Activities -2

Developing, teaching, and licensing CSIRT courses

- authorize trained instructors to deliver the suite of courses
- administer the CERT-Certified Computer Security Incident Handler certification license CSIRT courses to other external organizations
- license CERT® courses to SEI Partners, e.g.

CERT® CSIRT Courses

Creating a CSIRT [1 day]

- provides a high level overview of the key issues and decisions that must be addressed in establishing a CSIRT.

Managing CSIRTs [3 days]

- provides prospective or current managers with an overview of the incident handling arena including the CSIRT environment, organizational interactions, and the nature of incident management activities.

Fundamentals of Incident Handling for Technical Staff [5 days]

- provides basic introduction to the main incident handling tasks and critical thinking skills that incident handlers need to perform CSIRT functions

Advanced Incident Handling for Technical Staff [5 days]

- provides guidance incident handlers can use in responding to system compromises at the privileged level; participants identify and analyze a set of events and then propose appropriate response strategies through interactive instruction, facilitated discussions, and group exercises

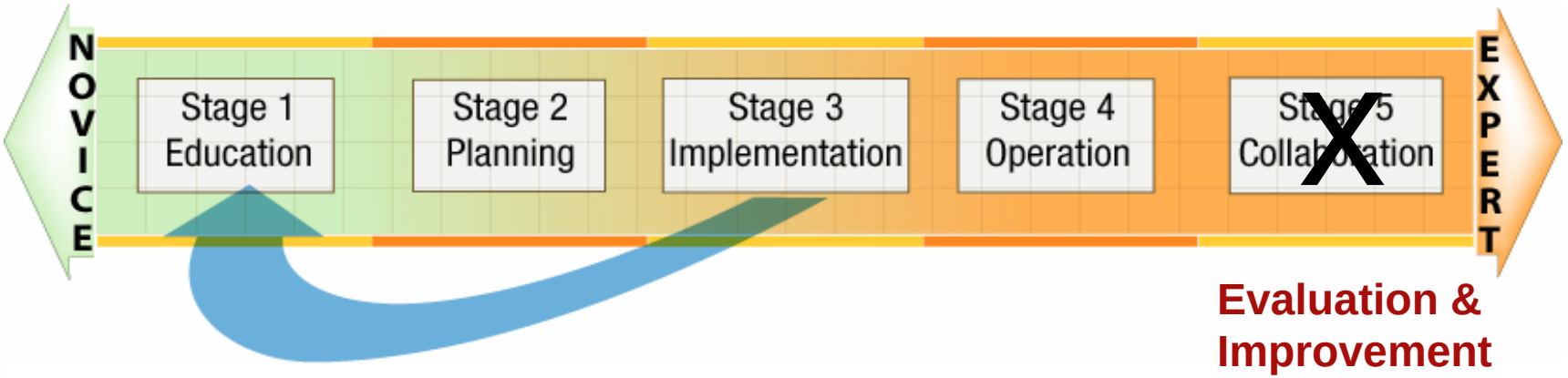
Community Projects

A sample of current CSIRT projects include

- IETF Incident Handling Working Group (INCH WG)
- IETF Intrusion Detection Working Group (IDWG)
- Automated Incident Reporting (AirCERT)
- System for Internet Level Knowledge (SiLK)
- Clearing House for Incident Handling Tools (CHIHT)
- Common Advisory Interchange Format (CAIF)
- The European Computer Security Incident Response Team Network (eCSIRT.net)
- Training of Network Security Incident Teams Staff (TRANSITS)
- Trusted Introducer for CSIRTs in Europe (commissioned by TERENA)

Approach for Developing a CSIRT

Stage 1	Educating the organization
Stage 2	Planning effort
Stage 3	Initial implementation
Stage 4	Operational phase
Stage 5	~~Peer collaboration~~ **Mature teams now focus on Evaluation & Improvement**



CERT

Some CSIRT Lessons Learned

Trustworthiness is paramount to success.

All CSIRTs differ in their mission and goals.

Most CSIRTs

- fail to plan for growth and are soon overwhelmed
- take 1-2 years to gain constituency recognition

CSIRTs should

- share information and knowledge as openly as possible
- set expectations repeatedly
- train for a marathon, not a sprint
- be proactive

Contact Information

CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA

Web: http://www.cert.org/

Email: cert@cert.org

Hotline: +1 412 268 7090
CERT personnel answer
08:00–17:00
EST(UTC-5)/EDT(UTC-4)
On call for emergencies
during other hours

CERT CSIRT Development Team
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213 USA

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

Email: csirt-info@cert.org