Software Engineering Institute

Department of Defense R&D Laboratory FFRDC
Created in 1984
Administered by Carnegie Mellon University
Headquartered in Pittsburgh, PA; offices and support worldwide
Strategy

Create usable technologies

Apply them to real problems

Amplify their impact by accelerating broad adoption
SEI Technical Programs

Networked Systems Survivability
- Survivable Systems Engineering
- Survivable Enterprise Management
- CERT Coordination Center
- Network Situational Awareness
- Practices Development and Training

Software Engineering Process Management
- Capability Maturity Model Integration
- Team Software Process
- Software Engineering Measurement and Analysis

Research, Technology, and Systems Solutions*
- Product Line Practice
- Software Architecture Technology
- Predictable Assembly from Certifiable Code
- Integration of Software-Intensive Systems
- Performance-Critical Systems
- Software Assurance

Acquisition Support

Other Research
- Independent R&D
- Mission Success in Complex Environments
- Ultra-Large-Scale Systems
- Software Assurance

* In 2008, the Research, Technology, and Systems Solutions was formed by the merger of the Product Line Systems and Dynamic Systems programs.
The Morris Worm, November 1988

1988 Internet

- 60,000 computers
- 6,000 hosts affected by worm
- NSFNET backbone upgraded to T1 (1.544Mbps)
- research and education oriented
- commercial use just beginning
- CERT/CC created

Robert Morris, Jr.; photo courtesy Computerworld.
In the beginning...

The SEI established, with DARPA sponsorship, the Computer Emergency Response Team Coordination Center in 1988.

The CERT/CC’s mission:

- respond to security emergencies on the Internet
- serve as a focal point for reporting & remediation of security vulnerabilities
- serve as a model to help others establish incident response teams
- raise awareness of security issues.
The original model

CERT System

INTERNET RESEARCH

MILNET

SPAN

BANKS...

DIRECTORY SERVICE

CCC - Constituency Coordinating Center
TCC - Technology Coordinating Center

UNIX EXPERTS

DECNET EXPERTS

PC EXPERTS

Hotline
The Model Was Adopted and Evolved
And we evolved too

Today’s Mission: To identify, develop, mature, and broadly transition new

- system development practices
- management practices
- system monitoring practices
- incident investigation practices

And technologies to protect the Nation’s critical systems and ensure they provide critical functionality and protect sensitive data, even in the face of attacks, accidents, and failures
Portfolio of Work

Protect

-- Vulnerability Discovery, Remediation & Alerts
-- Security Requirements Engineering
-- Secure Development & Coding Practices
-- Function Extraction for Software Assurance
-- Improved Systems & Security Management Practices

Detect

-- Network Situational Awareness: technologies, methods, studies, services
-- Malicious code: analysis methods & tools, studies, services
-- Threat identification: public and private source monitoring, alerts
-- Insider Threat: studies, mitigation practices, detection technology

Respond

-- Security Incident Response: direct support, practices, services
-- International response team development & coordination
-- Forensics: method & tool development, support to investigators

Workforce Development
Courses, curriculum materials, reference library, virtual training environment & lab, exercise network
CERT/CC Focus

People with malicious intent

Technologists

Asset Holders

Intel
Military
Law Enforcement
Homeland Security
Technical Staff
National CSIRTs
Financial & other industry

CERT Coordination Center
Services over Time

Decade 1: Capability Building
- Vendor Security Team Advocacy
- CSIRT Creation
- 10+ vendors Average Internet Site Focus
- Incident Response Team of Last Resort

Decade 2: Recognition of Risk
- Vulnerability Remediation
- 700+ vendors National/Economic Security Focus
- Major Internet Security Event Coordination

Decade 3: Protecting National & Economic Security
- Vul Discovery
- Secure Coding
- Forensics
- Artifact Analysis
- CSIRTs with National Responsibility
- National & Economic Security Incident Support

1988 1998 2008 2018
CERT/CC Principles

**confidentiality**
- reporting victims not identified without permission
- activity described without attribution

**impartiality**
- as FFRDC, not government or industry
- no reason to over- or understate issues

**value**
- bring technical expertise to solve hard technical problems

**coordination**
- academia/industry/government both domestic and international
- vendors regardless of market share/disclosure policies/development process maturity/source code availability
Vulnerability Analysis

Scope: Provide the primary analytical capability for analyzing vulnerabilities and disseminating information through the National Cyber Alert System.

Areas:

- **Technical analysis** - Perform technical analysis of vulnerabilities reported to gain insight into preconditions, impacts and scope.
- **Coordination** - Work with vulnerability reporters and vendors to understand, resolve and disclose vulnerabilities as appropriate.
- **Publication** - Develop and produce content for the National Cyber Alert System, which includes Technical Security Alerts, Security Alerts, and Vulnerability Notes.
- **Rapid communication channels** - Cultivate vendor relationships to ensure secure and rapid communication channels.
- **Vulnerability Discovery** – Take knowledge we learn from vulnerability analysis and apply it to help vendors reduce vulnerabilities in their products.