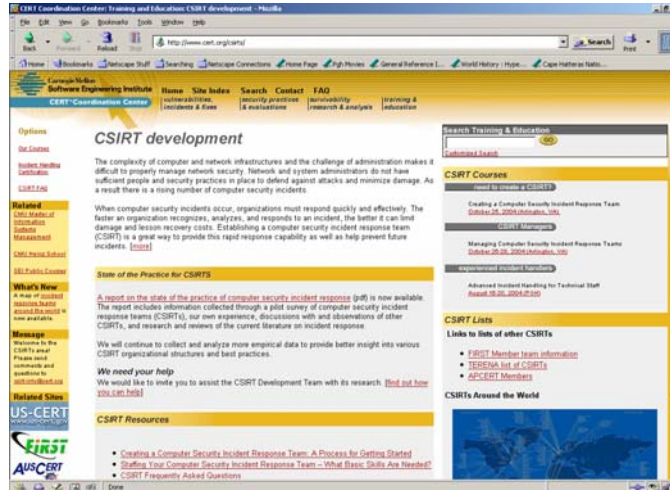




Who We Are: The CERT CSIRT Development Team (CDT)



<http://www.cert.org/csirts/>

© 2005 by Carnegie Mellon University

2

Software Engineering Institute

The CERT CSIRT Development Team is part of the CERT Education and Training area of the CERT® Program within the Software Engineering Institute

Our Vision and Mission

Vision

- Sufficient CSIRTs exist to meet the demand to protect the resources of the organizations they support

Mission

- Foster the growth of global incident management capabilities
- Assist commercial, governmental, educational, national and international organizations in establishing effective CSIRTs
- Help existing CSIRTs improve their services and operations through training, mentoring, and collaboration

What Do We Do? -1

As part of the SEI, the CERT CSIRT Development Team

- researches the current incident management environment, looking to synthesize existing information and best practices into guides, standards, and methodologies for performing incident handling processes and functions
- works with teams to
 - develop strategies to plan and implement CSIRTs
 - develop best practices for operating CSIRTs
 - adopt CSIRT policies and standard operating procedures
 - develop incident management publications, guides, templates, and checklists
- engages with customers to
 - assist in planning and designing incident management capabilities
 - assist in developing an implementation plan
 - evaluate and assess incident management capabilities

What Do We Do? -2

We also

- develop and teach courses related to CSIRTs
- license courses to organizations and train their trainers to deliver the materials
- provide a CERT-Certified Computer Security Incident Handler certification

CSIRT Related Courses

Courses we provide

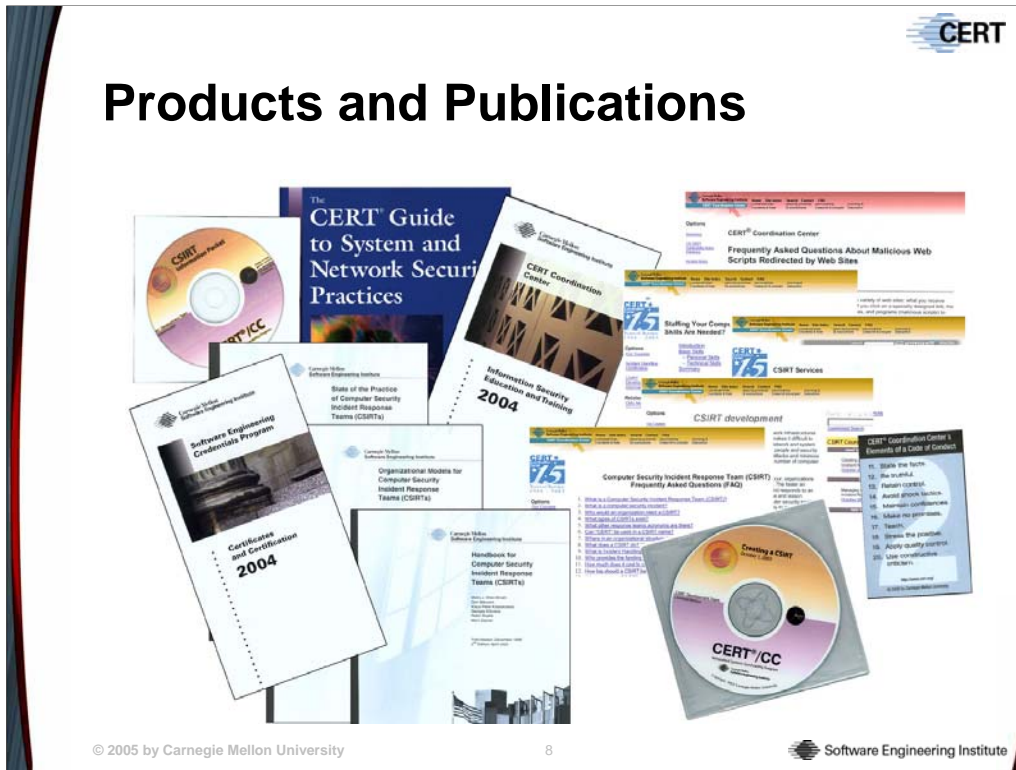
- Creating a CSIRT
- Managing CSIRTs
- Fundamentals of Incident Handling for Technical Staff
- Advanced Incident Handling for Technical Staff

CERT®-Certified Computer Security Incident Handler

Requirements for earning certification

- A three-course sequence from the SEI or its licensees (transition partners)
 - Information Security for Technical Staff (5 days) **or** Advanced Information Security for Technical Staff (5 days)
 - Fundamentals of Incident Handling (5 days)
 - Advanced Incident Handling (5 days)
- Three years of experience in the incident handling area (management and/or technical)
- Submission of application for certification and successful completion of the review process
- Letter of recommendation from current or previous manager
- Successful completion of evaluation administered by the Software Engineering Institute

Products and Publications



© 2005 by Carnegie Mellon University

8

Software Engineering Institute

The CERT CSIRT Development Team has created products based on the collective CERT/CC experiences in incident and vulnerability handling as well as artifact analysis.

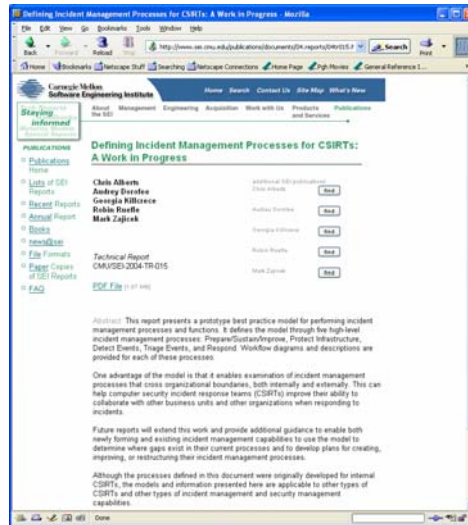
These products enable us to

- help organizations identify effective processes for incident management
- provide guidance to organizations for developing global CSIRT capabilities
- develop, promote, and expand best practices for CSIRTs
- identify transition partners for licensing CSIRT courses to broaden our global reach

Publications Include

- Handbook for CSIRTs
<http://www.cert.org/archive/pdf/csirt-handbook.pdf>
- Steps for Creating National CSIRTs
<http://www.cert.org/archive/pdf/NationalCSIRTs.pdf>
- CSIRT Services List
<http://www.cert.org/csirts/services.html>
- State of the Practice of Computer Security Incident Response Teams (CSIRTs)
<http://www.cert.org/archive/pdf/03tr001.pdf>
- Organizational Models for Computer Security Incident Response Teams
<http://www.cert.org/archive/pdf/03hb001.pdf>
- Staffing Your Computer Security Incident Response Team – What Basic Skills Are Needed?
<http://www.cert.org/csirts/csirt-staffing.html>

Defining Incident Management Processes for CSIRTs: A Work in Progress



<http://www.sei.cmu.edu/publications/documents/04.reports/04tr015.html>

© 2005 by Carnegie Mellon University

10

Software Engineering Institute

Since the release of this report we have evolved our thinking on incident management and its definition.

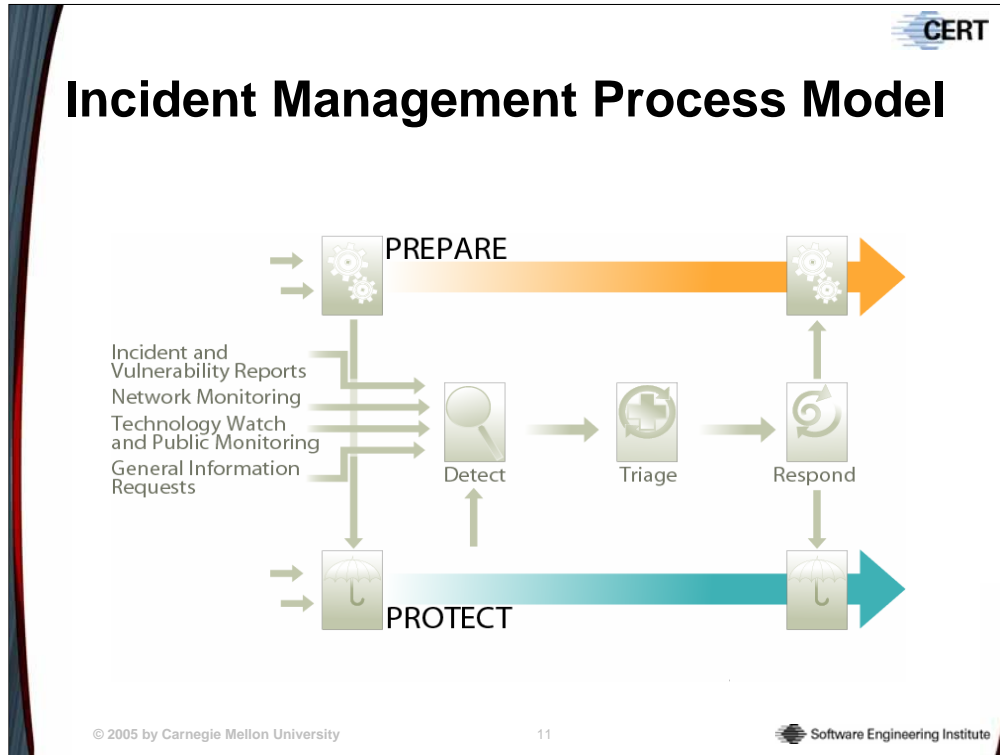
A computer security incident management capability is the ability to provide end-to-end management of computer security events and incidents.

For computer security incident response to occur in an effective and successful way, all the tasks and processes being performed must be viewed from an enterprise perspective. This means identifying how tasks and processes relate, how information is exchanged, and how actions are coordinated, no matter who is performing the work. Looking only at the response part of the process misses key actions that if not done in a timely, consistent, and quality-driven manner will impact the overall response, possibly delaying actions due to the confusion of roles and responsibilities, ownership of data and systems, and authority. Response can also be delayed or ineffective because of communications problems (not knowing whom to contact) and even due to poor quality information about the event or incident. Any impact on the response timeliness and quality can cause further damage to critical assets and data during an incident.

This bigger picture of activity is what is meant as incident management. Identifying and defining these interfaces and the roles and responsibilities of the various participants across the enterprise is a key part of setting up any incident management capability.

We define incident handling as one service that involves all the processes or tasks associated with “handling” events and incidents. Incident handling includes multiple functions: detecting, reporting, triage, analysis, and incident response.

Incident response, as noted in the list above, is one process, the last step, that is involved in incident handling. It is the process that encompasses the planning, coordination, and execution of any appropriate mitigation and recovery strategies and actions.



The CSIRT Development Team in the CERT Program has defined a “best practice” set of processes for incident management.

To do this we

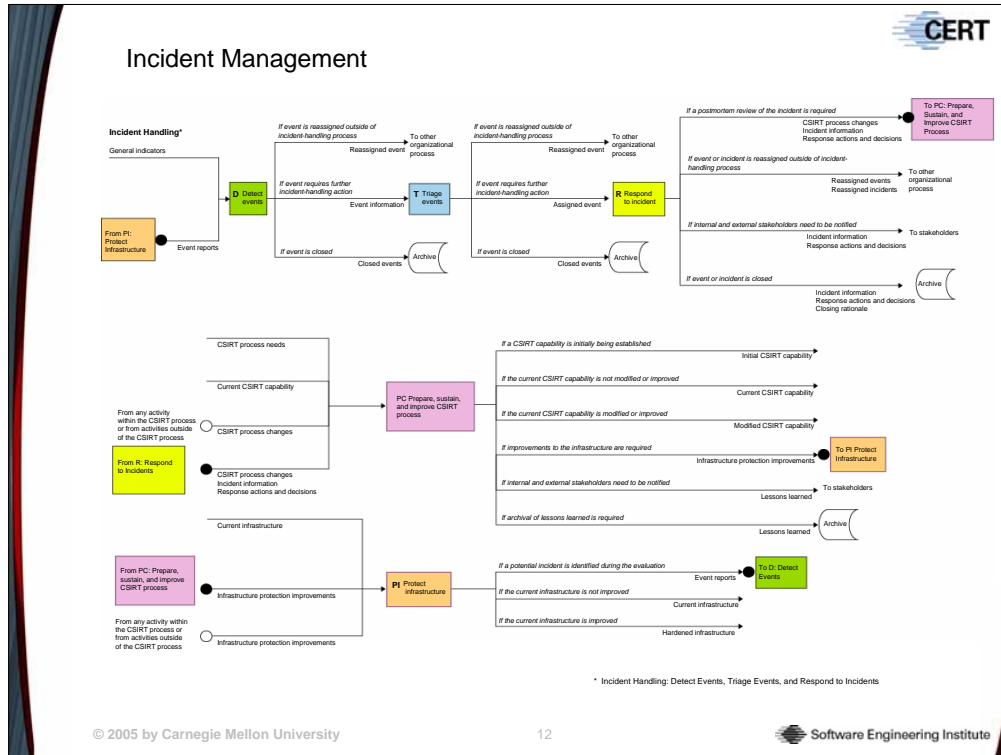
- determined processes
- outlined processes via workflow diagrams
- provided details and requirements of each process

This model is presented and described in SEI Technical Report CMU/SEI-2004-TR-015, Defining Incident Management Processes: A Work in Progress. This report is available at:

<http://www.cert.org/archive/pdf/04tr015.pdf>

This model documents a set of processes that outline various incident management functions. From this work a methodology for assessing and benchmarking an organization’s incident management processes can be developed. This methodology and resulting assessment instrument will enable teams to evaluate their incident management performance for the following processes:

- Prepare/Improve/Sustain (Prepare)
- Protect Infrastructure (Protect)
- Detect Events (Detect)
- Triage Events (Triage)
- Respond.



Responding to computer security incidents does not happen in isolation. Actions taken to prevent or mitigate ongoing and potential computer security events and incidents can involve tasks performed by a wide range of participants; this can include network and system administrators, human resources, public affairs, information security officers (ISOs), C-level managers (such as chief information officers [CIOs], chief security officers [CSOs], chief risk officers [CROs], and other similar types of managers) and even constituent representatives.

This question is one that is often asked by organizations as they plan their incident management strategy. They want to know what organizational units should be involved, what types of staff will be needed to perform the functions, and what types of skills that staff must have. They also want a way to identify what organizational units are already doing this type of work and want to understand the critical interfaces and interactions between different parts of the organization, different security functions, and the incident management process, in an effort to be able to build effective capabilities.

Incident management, then, is an abstract, enterprise-wide capability, potentially involving every business unit within the organization. As such, it is a subset of Security Management activities and functions, and therefore often crosses into and includes some general security tasks and practices.

Strategies for Building, Improving, or Evaluating Capabilities

Our Incident Management Model and Framework help organizations:

- define their As-Is or current state of incident management processes
- perform a gap analyses of their current state
- develop the To-Be or future state of their incident management processes—this is process improvement
- define processes, policies, procedures, and training needed to fill gaps and reach the To-Be state

Perform a traditional process gap analysis by looking for characteristics such as

- missing or poorly defined handoffs
- missing or poorly defined aspects of each process activity
- bottlenecks in the process
- poorly defined activity flows
- single points of failure

Current Projects

- Working with U.S. Federal Agencies to create a set of incident management metrics for process improvement based on DoD CNDS metrics
- Working with California State University (CSU) system to create a CSIRT Framework for their 23 campuses
- Working with others on developing incident management process improvement plans—just finished a gap analysis
- Course Redesign: Fundamentals and Advanced Incident Handling courses—over the next six months
- Updating the CSIRT services list and corresponding documents (e.g., the Organizational Models document)
- Delivering approximately 20+ classes over the next 18 months

For More Information

CERT® CSIRT Development Team

CERT® Centers

Software Engineering Institute

Carnegie Mellon University

Pittsburgh, PA 15213 USA

+1 412 268 7090

csirt-info@cert.org

<http://www.cert.org/training/>

<http://www.cert.org/csirts/>