

New CERT[®] Certification to Train Computer Security Incident Handlers

Eric Hayes

Most organizations today depend on networked computer systems as an integral part of their businesses. As applications become more complex and services become increasingly integrated, protecting network security and recovering from computer security incidents has become a business-critical component of an organization's IT security plan. Creation of computer security incident response teams (CSIRTs) is an organizational best practice for protecting information assets and ensuring that an organization's mission survives. New laws and regulations also require organizations to identify and implement response capabilities—in some cases mandating that such incident response teams be formalized.

The CERT Coordination Center (CERT/CC) has been in the business of Internet security since 1988, handling incidents and helping other organizations create incident response teams. To help ensure a supply of qualified personnel to meet the growing demand for organizational incident response teams, the CERT/CC has created a program to train and certify individuals as CERT-Certified Computer Security Incident Handlers. CERT certification provides a tangible recognition of skills from the Internet's first and best-known computer security incident response team.

Certified incident handlers will be trained to handle diverse aspects of incident response and team leadership, ranging from applying operational concepts to managing a team to using technical expertise to prepare for, detect, analyze, and respond to security events. This range of knowledge ensures that CERT-certified incident handlers are well prepared to recognize and respond to security risks and threats.

The Curriculum

The certification requires individuals to take four core courses from the SEI or from an SEI transition partner (an organization licensed to provide SEI courses):

1. Creating a Computer Security Incident Response Team (CSIRT) (one day)
2. Information Security for Technical Staff (five days)
3. Managing CSIRTs (three days) or Fundamentals of Incident Handling (five days)
4. Advanced Incident Handling (five days)

One elective course in computer forensics, intrusion detection and analysis, or security audits and assessments is also required. This requirement is met by completing a course at a university or college accredited by the Accreditation Board for Engineering and Technology (ABET) or by completing five continuing education units from a recognized security training organization.

Once the prerequisites and course curricula have been completed, a final requirement for certification is to pass an SEI-administered written exam. The certificate is valid for three years; renewals require additional continuing education units and experience in the field.

Qualifications for Applicants

Applicants need to have at least three years of technical or managerial experience in incident handling (IH). After applicants meet this basic prerequisite, they must submit a letter of recommendation from their current or previous manager in support of their application.

The program welcomes incident handlers, CSIRT managers, system and network administrators with IH experience, and IH trainers and educators, as well as those with some technical training who want to enter the IH field.

Benefits of Certification

The certification should help computer-security professionals in their careers by demonstrating that they have achieved a high level of expertise. Organizations that hire CERT-Certified Computer Security Incident Handlers will benefit by having employees who are able to

- identify the benefits, challenges, and operational requirements needed to successfully create a structured incident handling or management team
- successfully participate as leaders or members of CSIRTs
- describe the information security tenets of confidentiality, availability, and integrity, and apply these concepts to the protection of information and information assets in an enterprise using a variety of technical and procedural solutions
- recognize and identify organizational risks and threats
- recommend and implement best practices for incident handling functions, computer security solutions, and mitigation strategies to reduce risks and counter threats across the enterprise
- demonstrate technical expertise in analyzing incident data and identifying response strategies

The SEI invites all qualified applicants to consider the CERT-Certified Computer Security Incident Handler certification program to enhance their computer security careers.

For a directory of organizations that teach SEI courses, see the SEI transition partner Web site: <http://www.sei.cmu.edu/collaborating/partners/?si>

For more information, contact—

Kimberly Lang

Phone

412-268-9564

Email

training-info@cert.org

World Wide Web

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