



COURSE DETAILS

INTENDED AUDIENCE

New CSIRT members, other technical staff, and anyone interested in incident handling functions and activities.

LENGTH

Five Days; Days 1-4 (0900-1700) Day 5 (0900-1500)

COST

\$2499 including course notebook and course CD. Refreshments and catered lunch provided.

PREREQUISITES

None; however attendees should have some familiarity with basic networking concepts and Windows or Unix system administration.

This course may also be offered by arrangement at customer sites. Contact Outbreak Security for further information.

Outbreak Security

7 West Queens Way
Hampton, VA 23669 USA
1.757.265.0891

www.outbreaksecurity.com

FUNDAMENTALS OF INCIDENT HANDLING

Overview:

This five-day course, developed by the Software Engineering Institute at Carnegie Mellon University, is for computer security incident response team (CSIRT) technical personnel with little or no incident handling experience. It provides a basic introduction to the main incident handling tasks and critical thinking skills that will help an incident handler perform their daily work. It is recommended to those new to incident handling work.

The course is designed to provide insight into the type and nature of work that an incident handler may perform. It will provide an overview of the incident handling arena, including CSIRT services, intruder threats, and the nature of incident response activities. This course is part of the curriculum for the CERT-Certified Incident Handler program.

To maximize learning, the course is composed of both instructor lectures and significant class exercises.

Topics Include:

- The CSIRT environment
- CSIRT code of conduct
- Tools for CSIRT operations
- Obtaining Critical Information
- Recognizing signs of attacks
- Detecting and analyzing incidents
- Finding contact information
- Coordinating response
- Disseminating information
- Email and malicious code attacks
- Working with law enforcement

Objectives:

This course will help participants to recognize the importance of following well-defined processes, policies, and procedures; understand the technical, communication, and coordination issues involved in providing a CSIRT service; critically analyze and assess the impact of computer security incidents; effectively build and coordinate response strategies for various types of computer security incidents

About Outbreak:

Outbreak Security was established in 2007 by four distinguished information security professionals whose operational and executive information security and incident handling experience in the government, military, and private sector dates back to 1988 and the birth of the incident response community. Outbreak's instructors are also Visiting Scientists at the Software Engineering Institute at Carnegie Mellon University and have taught numerous incident handling courses there for the CERT/CC.

Instructor biographies and corporate information may be found at www.outbreaksecurity.com.