



COURSE DETAILS

INTENDED AUDIENCE

Current & Prospective CSIRT Managers and Members; CIOs and other managers or executive leaders involved with incident handling functions

LENGTH

Three Days; 0900-1700

COST

\$1499 including course notebook, resources, and course CD. Refreshments and catered lunch provided.

PREREQUISITES

None; however attendees may consider attending the one-day "Creating a CSIRT" class scheduled the day prior to this seminar.

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

MANAGING COMPUTER SECURITY INCIDENT RESPONSE TEAMS

Overview:

This three-day course, developed by the Software Engineering Institute at Carnegie Mellon University, is designed for managers and project leaders responsible for coordinating CSIRT operations. The course provides insight into the type and nature of the work that CSIRT staff may be expected to handle. The course also provides prospective or current managers with an overview of the incident handling process and the types of tools and infrastructure needed to be effective.

The course incorporates interactive instruction, exercises, and role playing. During a simulated incident, attendees will gain experience with the type of decisions they might face on a regular basis. Technical issues are discussed from a management perspective and attendees are not required to have significant technical knowledge to benefit from the course.

Topics Include:

- CSIRT management issues
- The CSIRT environment
- Staffing issues
- CSIRT Code of Conduct
- Media issues
- Managing the CSIRT infrastructure
- Critical information
- Managing a CSIRT hotline
- Conducting Triage
- Coordinating response
- Handling major events
- Prioritizing and load balancing
- Publishing information
- Working with law enforcement

Objectives:

This course will help participants to recognize the importance of establishing well-defined policies and procedures for incident management processes; identify policies and procedures that should be established and implemented for a CSIRT; understand incident management activities, including the types of activities and interactions that a CSIRT may perform; learn about various processes involved in detecting and responding to computer security events and incidents; identify key components needed for protecting and sustaining CSIRT operations; manage a responsive, effective team of computer security professionals.

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.