



COURSE DETAILS

INTENDED AUDIENCE

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

LENGTH

One Day; 0900-1700

COST

\$499, including course notebook, CSIRT action plan, and course CD. Refreshments and catered lunch provided.

PREREQUISITES

None.

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

CREATING A COMPUTER SECURITY INCIDENT RESPONSE TEAM

Overview:

This one-day course, developed by the Software Engineering Institute at Carnegie Mellon University, is designed for managers and project leaders who have been tasked with implementing a computer security incident response team (CSIRT). This course provides a high level overview of the key issues and decisions that must be addressed in establishing a CSIRT. As part of the course, attendees will develop an action plan that can be used as a starting point in planning and implementing their own CSIRT.

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

Topics Include:

- Incident management
- Planning a CSIRT
- Creating a CSIRT vision
- CSIRT objectives and authority
- CSIRT organizational issues
- Range and levels of Services
- Funding issues
- Hiring and training CSIRT staff
- CSIRT policies and procedures
- CSIRT infrastructure requirements
- Operational issues and strategies
- Collaboration and communication

Objectives:

This course will help participants to understand the requirements for establishing an effective CSIRT; strategically plan the development and implementation of a new CSIRT capability; highlight issues associated with assembling a responsive, effective team of computer security professionals; identify policies and procedures that should be established and implemented; understand various organizational models for a new CSIRT; understand the variety and level of services that can be provided by a CSIRT.

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.