



## COURSE DETAILS

### INTENDED AUDIENCE

Current & Prospective CSIRT Managers and Members; other technical staff involved with incident handling activities.

### LENGTH

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

### COST

\$2599 including course notebook and course CD. Refreshments and catered lunch provided.

### PREREQUISITES

It is recommended that attendees have a moderate understanding of network protocols, basic programming concepts, and previous incident handling experience.

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](http://www.outbreaksecurity.com)

# ADVANCED INCIDENT HANDLING FOR TECHNICAL STAFF

## Overview:

This five-day course, developed by the Software Engineering Institute at Carnegie Mellon University is designed for experienced CSIRT technical personnel to address techniques employed in detecting and responding to current and emerging computer security threats and attacks that are targeted against a variety of operating systems and architectures.

Participants work as a team throughout the week to handle a series of escalating incidents that are presented as part of an ongoing scenario. Work includes team analysis of information and presentation of findings and response strategies. Participants also review broader aspects of CSIRT work such as artifact analysis; vulnerability handling; and the development of advisories, alerts, and management briefings. 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:

- Responding to common attacks
- Understanding intruder toolkits
- Handling major events and incidents
- Artifact analysis in incident handling
- Fundamental vulnerability causes
- Vulnerability handling
- Publishing CSIRT information
- Security case study

## Objectives:

This course will help participants to detect and characterize various attack types; gain a practical understanding of various methods for analyzing artifacts left on a compromised system; understand the complexity of and effectively respond to privileged and major events and incidents within your CSIRT; obtain practical experience in the analysis of vulnerabilities and the coordination of vulnerability handling tasks; formulate effective advisories, alerts, and management briefings

## 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](http://www.outbreaksecurity.com).