



COURSE DETAILS

INTENDED AUDIENCE

Current & Prospective CSIRT Managers and Members; technical staff and managers involved with managing or supporting networked information systems.

LENGTH

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

COST

\$2599 including course notebook and course CD. Additional Lab Fee of \$250 includes student use of all PC and software required for the class. Refreshments and catered lunch provided.

PREREQUISITES

None; however attendees should be familiar with the ISO/OSI model, Ethernet, TCP/IP, and modern operating systems such as Windows 2000/XP or Unix.

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

INFORMATION SECURITY FOR TECHNICAL STAFF (ISTS)

Overview:

This five-day course, developed by the Software Engineering Institute at Carnegie Mellon University, is designed to provide participants with practical techniques for protecting the security of an organization's information assets and resources, beginning with concepts and proceeding on to technical implementations.

The principles, strategies, and practices covered are applicable to most system platforms and network environments. To illustrate important concepts and security technologies, demonstrations and multiple hands-on exercises will include implementations applicable to Linux and Windows systems as well as Cisco networking equipment. This course is part of the curriculum for the CERT-Certified Incident Handler Program.

Topics Include:

- The challenge of survivability
- Asset and risk management
- Forming and Implementing Policy
- Security Knowledge in Practice
- TCP/IP security
- Cryptography
- Information gathering
- Threats, vulnerabilities, and attacks
- Host system hardening
- Securing network infrastructure
- Deploying firewalls
- Securing remote access
- Intrusion detection systems

Technical Activities:

Hands-on labs and demonstrations include subjects such as: Scanning and enumeration; Enigmail and Mozilla Thunderbird email client use of the OpenPGP standard; Windows Group Policy and Security templates; securing remote access with IPSec; assessing networks with Nessus; intrusion detection and prevention with Snort; as well as information on personal and enterprise firewalls, password cracking, and extensive hacking/hardening of Linux, Windows, and Cisco platforms in both wireless and cabled networks. Each student will have the use of a laptop for the duration of the course, as well as access to a wide variety of networked systems.

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.