

# Fundamentals of Incident Handling

## *“Can your incident response team meet the challenge?”*

Most organizations are not prepared to deal with network attacks and intrusions. They only realize the need to prepare for incidents and respond to them after they are hit by an attack. As a result, when an intrusion occurs, organizations frequently make hasty decisions that reduce their ability to survive and recover from an incident.

### Course Overview

This five-day course gives information technology security staff a comprehensive overview of the issues and procedures for handling security incidents. The course also familiarizes attendees with the types of work an incident handler performs.

Fundamentals of Incident Handling is taught by one of the most prominent Network Security and Incident Response experts in the world, Dr. Klaus-Peter Kossakowski. He will share insights from his years of experience creating and working with incident response teams worldwide. Dr. Kossakowski was the first one to license the course source material from the CERT Coordination Center and has adapted it for an international audience.

### Who Should Attend?

This course benefits prospective and new incident response staff seeking to learn and improve their incident response skills. It also benefits managers who wish to deepen their understanding of incident response issues. Suggested prerequisites include basic familiarity with Internet services and protocols and experience with system administration for Windows NT/2000, UNIX, or Linux systems.

After taking this course, participants often contact Dr. Kossakowski and his associates to arrange workshops and individual training sessions at their workplace to focus on advanced topics in incident response.

### Course Objectives

#### **This course will help technical staff understand how to:**

- Gather the information necessary to characterize an incident
- Analyze a variety of security incidents
- Recognize and respond to incident attacks
- Avoid common mistakes in incident response
- Communicate and coordinate incident response services internally and externally



forensic

malicious code

computer  
attack security

network security intrusion  
CERT

## Course Topics

### The course covers the following topics:

- Strategies for incident response
- Overview of scans, probes, and intruder attacks
- Working with other incident response team members
- Techniques for gathering, tracking, and categorizing incident information
- Analyzing incident reports
- Handling common attacks such as email spoofing or spamming, denial of service attacks, and malicious code
- Coordinating organizational response
- Cryptographic and data security issues

Dr. Kossakowski uses interactive instruction, exercises, and role-playing to teach participants how to respond to security incidents.

### Company Description

PRESECURE provides consulting to senior managerial and technical staff about improving computer and network security as well as incident response. The company draws from an international group of experienced network security professionals who can provide ongoing support before, during, and after security incidents.

### In the area of incident response PRESECURE can help you:

- Identify security events such as attacks or attempted intrusions
- Understand and execute appropriate responses
- Identify new and existing threats and vulnerabilities

### Course Availability

PRESECURE holds periodic sessions of this course in North America and Europe. For current course offerings, visit: <http://www.pre-secure.com/courses/>

Please send email to [irt@pre-secure.com](mailto:irt@pre-secure.com) if you would like to register for a course.

Dr. Klaus-Peter Kossakowski is also available to teach the Fundamentals of Incident Handling at your site. Please send email to [kpk@pre-secure.com](mailto:kpk@pre-secure.com) if you are interested in this option.

#### How to contact us:

PRESECURE Consulting GmbH  
P.O. Box 141  
48283 Telgte  
Germany  
Tel. +49-2504-729-337  
Fax +49-2504-729-420  
Email [irt@pre-secure.com](mailto:irt@pre-secure.com)  
<http://www.pre-secure.com>

*PRESECURE® is a trademark of PRESECURE Consulting GmbH. All other trademarks and service marks remain the property of their respective holders and are hereby acknowledged.*

intrusion  
network security  
CERT  
malicious code

PRESECURE