

Managing Computer Security Incident Response Teams (CSIRTs)

“Can you business survive and recover from network attacks and intruder threats?”

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 three-day course gives managers a detailed picture of many primary challenges that arise in leading an incident response team and then reveals time-tested techniques and solutions for effectively dealing with them.

The course 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 CSIRTs worldwide. Dr. Kossakowski was the first one to license the source material from the CERT Coordination Center and has adapted it for an international audience.

Who should attend?

The course benefits people who want to understand how incident response teams work and the issues they face. Past attendees have included information technology managers, constituents, media-relations staff, legal counsels, as well as senior managers. Many participants build on this course by taking Computer Security Incident Handling, an introductory five-day course. It is designed to deepen team members' knowledge of the skills and methods needed to better operate the daily activities of an incident response team. By taking the course attendees can effectively learn to train their own team and understand the more operational issues their team faces.

Course Objectives

After taking this course, you will understand the requirements for establishing an effective incident response team and be familiar with a wide range of incident response team goals, challenges, techniques, and solutions. During a simulated response to an incident, Dr. Kossakowski uses interactive instruction and role-playing techniques to help you experience the situational decisions you may encounter working on an incident response team. After attending this course, you will:

- Understand incident response issues, tools, and major strategies available
- Be familiar with the variety of services incident response teams can offer
- Realize what it takes to manage an effective and responsive team
- Identify essential incident response team policies and procedures

network security

attack

computer security

intrusion

CERT

Course Topics

The course offers a realistic look at the range of work incident response teams engage in daily. Important topics covered include:

- Communication inside and outside the incident response team
- Cryptographic and data protection issues
- Incident response team management issues such as hiring and media relations
- Incident response team work environment
- Forum of Incident Response and Security Teams (FIRST)
- Hotline and triage functions
- Incident response practices and strategies
- Information gathering methods
- Setting task priorities and balancing workloads
- Vulnerability assessment and intruder threats

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 if you would like to register for a course.

If your organization needs to focus on a particular topic in incident response or team development, Dr. Kossakowski will tailor a course or workshop to your needs by arrangement. Please send email to 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
<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