

## Implementing an Incident Response Strategy: Hands-On - 4 Days

### Conducting Forensics on Windows

*Course 536 Overview*

- You Will Learn How To**
- Implement a computer forensics incident-response strategy
  - Lead a successful investigation from the initial response to completion
  - Conduct disc-based analysis and recover deleted files
  - Identify information-hiding techniques
  - Reconstruct user activity from e-mail, temporary Internet files and cached data
  - Assess the integrity of system memory and process architecture to reveal malicious codes

**Course Benefits** Do you know what to do if your organisation's security is compromised? Threats of computer crime against an organisation's infrastructure have grown substantially, but there are steps you can take. In this course, you apply the latest Windows-based computer forensic techniques to uncover illicit activity and recover lost data. Every crime leaves behind clues. With the right tools, you can effectively respond to and counteract security threats.

**Who Should Attend** Systems administrators and those involved in responding to security incidents. Knowledge of Windows-based PCs, including hardware and operating system software, at the level of Course 2400, "Windows 7 Comprehensive Introduction", is assumed

**Hands-On Training** Exercises, providing experience using software forensic tools to investigate Windows-based systems, include:

- Leveraging case-management software
- Employing forensic toolkits
- Imaging digital media
- Hiding and discovering potential evidence
- Applying steganography techniques
- Manipulating alternate data streams
- Discovering information in mangled files
- Conducting e-mail investigations
- Reconstructing browser and web server activity
- Establishing covert surveillance with keystroke loggers and remote access
- Configuring tools to detect a rootkit

## Implementing an Incident Response Strategy: Hands-On - 4 Days

### Conducting Forensics on Windows

#### Course 536 Outline

#### Introduction to Computer Forensics

- Responding to incidents
- Applying forensic analysis skills
- Distinguishing between unpermitted corporate and criminal activity

#### Handling Preliminary Investigations

##### Planning for incident response

- Knowing your organisation's policies
- Minimising impact on your organisation

##### Identifying the incident life cycle

- Performing incident analysis
- Capturing volatile information

#### Controlling an Investigation

##### Collecting digital evidence

- Chain of custody and process integrity
- Advantages of the forensics analysis team

##### Legal aspects of acquiring evidence

- Securing and documenting the scene
- Processing and logging evidence

#### Conducting Disk-Based Analysis

##### Forensics lab operations

- Acquiring a bit-stream image
- Enabling a write blocker
- Establishing a baseline
- Physically protecting the media

##### Disk structure and recovery techniques

- Disk geometry components
- Inspecting Windows file system architectures
- Locating and restoring deleted content

#### Investigating Information-Hiding Techniques

##### Uncovering potential cybersecurity threats or leaks

- Scanning and evaluating alternate data streams
- Executing code from a stream
- Steganography tools and concepts
- Detecting steganography
- Scavenging slack space

##### Inspecting header signatures and file mangling

- Combining files
- Binding multiple executable files
- File time analysis

#### Scrutinising E-mail

##### Investigating the mail client

- Interpreting e-mail headers
- Recovering deleted e-mails

##### Validating e-mail header information

- Detecting spoofed e-mail
- Verifying e-mail routing

#### Tracing Internet Access

##### Inspecting browser cache and history files

- Exploring temporary Internet files
- Researching cookie storage
- Reconstructing cleared browser history
- Assessing antiforensics features browsers
- Updated browser analysis

##### Auditing Internet surfing

- Tracking user activity
- Uncovering unauthorised usage

#### Searching Memory in Real Time

##### Comparing the architecture of processes

- Identifying user and kernel memory
- Inspecting threads
- Discovering rogue DLLs and drivers

##### Employing advanced process analysis methods

- Evaluating processes with Windows Management Instrumentation (WMI)
- Walking dependency trees

##### Auditing processes and services

- Investigating the process table
- Discovering evidence in the Registry
- Deploying and detecting a rootkit

##### Implementing covert surveillance techniques

- Logging key strokes
- Observing real-time remote desktops
- Monitoring Internet access