

Computer Incident Response

Introduction

This course addresses the relevant components in any computer incident environment as it applies to criminal or civil matters. It is an essential course for the first responder and the computer forensic engineer who conducts or processes digital investigations within the corporate and legal environment.

Aim

The aim of this module is to provide delegates with a sound knowledge and understanding to enable them to investigate secure and recover admissible evidence from computers and digital devices. Acquire the skills and competencies to prepare such evidence for presentation in a Court of Law. This course will assist the delegate who wishes to proceed to the other courses on computer forensic evidence investigation.



Preliminaries

- Computer security
- Computer incident
- Incident response

What is a Computer

- Varied definitions
- Scope of definitions
- Summary of definitions
- Computer devices
- Parts of a computer
- Computer storage technologies

Computer evidence

- Characteristics of computer evidence
- Volatile and non volatile data
- Computer storage technologies

Architecture of a Computer Network

- Standalone Computer
- Computer Network
- Computer operating Systems
- Computer peripherals

Computer incident – Classification

- What constitutes a Computer incident?
- Misuse – Security breach – operational mishaps

Misuse – Corporate environment

- Email abuse
- Resource access
- Privilege hijack – shoulder surfing
- Internet surfing

Security breach

- What constitutes a security breach
- Classification of breach – (Internal / External)
- Objects of the breach
- Targets of the breach – Files, Repositories, Web sites
- Workstation, Servers, Routers, Switches, Hubs, PDA & Mobile phones

Incident Response

- Summary of above
- What Constitutes response to an incident
- Traditional forms of response
- The Bigger picture with response – Corporate security
- Possible civil litigation and criminal prosecution

How to conduct an incident response

- Securing the scene
- Victim interview process
- Preliminary concerns ~ Data protection
- Human rights - Privacy
- The need for a response Team – Proactive placement
- Membership of the Team
- Legal preliminaries – Formulation of User policy
- Log on scripts, templates, employment conditions
- Documenting delegated authority

Manual v. Automated investigation / response

- Preliminaries – Note taking, securing evidence, evidence integrity
- Incident scene – Locards principle usb, Pasted Notes, Cd, Floppy, DVD, digital cameras, cctv cameras, laptop switch, hub, external drives.
- Fire brigade approach / Documented approach
- Do's and Don'ts ~ Log files , MAC modification, Bios modification
- Tipping off, Power off or plug off, Screen image.
- Volatile and Non volatile resources need to secure volatile data.
- Manual – incident response, available personnel dictates approach/ Complexity of response. Check device logs, event viewer, registry processes, resource access, open files.
- Automated – incident response ~ level of personnel skill, available software, standalone or remote subject, time factor, cost.

Best Practice

- Need for proactive measures – Team, existing protocol,
- Criminal incident – to report or not to report?
- Cost of non compliance with protocol – Case law examples and legislation examples
- Corporate Governance and Compliance WorldCom, Arthur Anderson, Sox, Card industry, HIPPA, Companies Act as amended
- Need for IT Audit and Gap analysis
- ACPO and Sedona Principles

Course Review / Questions

Intended Learning Outcomes

On successful completion of this module a delegate will be able to:

Knowledge

- Recognise the different components that are required for setting up an incident response team.
- Design and implement a protocol for computer incident response within a corporate environment.
- Secure the incident scene and assist in the investigation of a digital incident environment
- Understand what is required during testimony in court