

Symantec™ Incident Handling and Response

Course Description

This comprehensive three-day workshop provides an overview of corporate incident handling and response and its impact on the organization. Concepts presented include incident handling and response planning, identifying and building an incident handling and response team, computer evidence preservation, business continuity and forensic readiness. The course provides an overview of the business value of a coordinated response strategy and outlines how to build a road map for designing and developing an incident handling and response program, including key elements of forensic readiness. The course also includes data acquisition techniques, rootkits and investigation tips. Lectures cover theoretical techniques, legal aspects, incident costs, and trends in incident handling and response. Practical techniques for addressing common scenarios are also covered.

Who Should Attend?

This course is designed to facilitate maximum exposure and awareness of the incident response process to all relevant business units.

Day 1 is designed for senior management, corporate security officers, IT management and system administrators plus management from other related business areas such as public relations, finance, human resources and legal personnel.

Day 2 follows on from Day 1 and is designed for corporate security officers, IT management and system administrators plus other parties interested in the more technical aspects of the incident handling and response process.

Learn How To:

- Assess and plan for how incidents affect the business
- Practically identify, handle and record incident response

- Structure a suitable incident handling and response team
- Ensure organizational readiness for effective response
- Put into practice the processes and methodologies of computer evidence collection
- Apply the principles of forensic analysis
- Identify appropriate resources, strengths and weaknesses
- Apply mitigation and restoration principles

Course Outline

This three-day course has both lecture and lab components. Course hours are 9:00 AM to 5:00 PM.

Day 1

Introduction

- Incident Types
- Incident Management Phases

Legal Framework

- Why is This Relevant?
- Overview of Current Acts and Regulations
- Acceptable Use Policy

Computer Forensics and Digital Evidence Awareness

- Definition of Computer Forensics
- Types of Digital Evidence and Characteristics
- Disks, Tapes and Other Media
- Live Data and Deleted Data
- Associated Evidence

Incident Response Teams

- Client Relationships
- Team Services, Types and Roles
- Using External Teams
- Preparation, Meetings and Questions

Incident Costs

- Simple Incident Costs
- Opportunity Costs

- Reducing Costs of Incidents
- Call and Escalation Tree
- Communication Methods
- Forensic Acquisition Kit Investment
- Procedures

Forensic Readiness

- Theory and Benefits
- Using Forms to Provide Chain of Evidence
- Log File Advice and Management
- Host/Networking Monitoring
- Maintaining an Inventory
- Forensics Laboratory Requirements
- Outsourcing Options

First Response

- Reporting Methods
- Logging and Auditing
- User/Help Desk Reports
- IT/System Problem Reports
- PR/Media Involvement
- Call Tree

Day 2

Technical Aspects of Incident Handling and Response

Detection Systems

- Intrusion Detection and Prevention System Types
- Log Types
- Log Processing Tools
- Log File Advice and Best Practices

Incident Scope Assessment

- Strategy Meeting
- Scoping With Caution
- Information Recording
- Log Processing
- Basic Host Analysis
- Timelines
- Keyword Searching
- Previewing a Disk

- Rootkits and Hidden Files
- Rootkit Detection Techniques
- Information Gathering

Principles of Digital Evidence Collection

- ACPO Principles
- Incident and Scene Containment
- Acquisition Guidelines
- System Shutdown Guidelines
- Evidence Handling and Transportation
- Using Chain of Evidence Forms
- Note Taking Tips
- Checklist

Volatile Evidence Collection

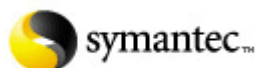
- Volatile Data Acquisition
- Windows Volatile
- UNIX Volatile

Static Evidence Collection

- Static Data Acquisition Principles
- Methodology and Tools
- Shutdown Considerations
- Acquiring Over the Network
- Removing Suspect Drives
- Installing Target Acquisition Drives
- Image File Destination Options
- Acquiring to a Disk File or Raw Disk
- Imaging Issues
- Linux/Solaris/Windows Variants
- Specialist Hardware and Software

Incident Handling and Response

- Isolation and Mitigation
- Additional Monitoring
- External Notifications
- Restoring and Securing the Systems
- Summary Meeting
- Policy and Procedure Review



Day 3

Practical Review of Incident Handling and Response Processes and Procedures

Lab Workshop

- Working Through the Incident Response Processes and Procedures
- Handling Various Types of Incidents
- Tracing, Tracking, Logging and Chain of Evidence Reporting
- Acquisition, Analysis and Conclusions

More information

Visit our Web Site

<http://ses.symantec.com/securitylearning>

Contact a Security Learning Services specialist

US toll-free 1 866 271 8200

securitylearning@symantec.com

About Symantec

Symantec is the global leader in information security providing a broad range of software, appliances and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure.

Symantec's Norton brand of products is the worldwide leader in consumer security and problem-solving solutions.

Headquartered in Cupertino, Calif., Symantec has operations in more than 40 countries. More information is available at www.symantec.com

Symantec World Headquarters

20330 Stevens Creek Blvd.

Cupertino, CA 95014 USA

1 408 517 8000

1 800 721 3934

www.symantec.com

