Forensics and Incident Response

Education Services Training Course

The Forensics and Incident Response Education (FIRE) course offered by Foundstone® Services is a defensive weapon to help you normalize your environment after a negative event has occurred. Hackers and disgruntled employees are using sophisticated tools and backdoor programs to steal your intellectual property and expose sensitive information—and they can cover their tracks in the process. In this course, we provide you with the forensic techniques to identify, respond to, and recover from both an insider and outsider attack. This comprehensive, technically detailed course enables you to successfully respond to incidents and reinforces your security posture.

Audience

System and network administrators, corporate security personnel, auditors, law enforcement officers, and consultants responsible for investigating network intrusions

Course Goals

- In-depth study of the computer forensics process
- Create evidentiary disk images
- Respond to unlawful access and information theft
- Incident response procedures for Unix and Windows

Agenda at a Glance

- Introduction
- Preparation
- Malware Strategies
- Windows Incident Response
- File Carving and Email Analysis
- Hash and Timeline Module
- Network-Based Monitoring
- Memory Forensics
- Unix and Linux Incident Response

Course Outline

Module 1—Introduction

- Overview of Course Content and Format
- Principles of Forensics and IR

Module 2—Preparation

- Data Collection Techniques
- Forensic Hardware
- Chain of Custody
- Basic Incident Response Process
- Pre-Incident Preparation
- Documentation Requirements

Module 3—Malware Strategies

- Common Approaches
- Containment and Remediation Strategies
- Malware Footprints

Module 4—Windows Incident Response

- Data Volatility
- Installed Software and Hotfixes
- Persistence Mechanisms
- Windows Audit Policies
- Malware Analysis
- Prefetch Analysis
- The Windows Registry
- Windows Event Log Analysis

Module 5—File Carving and Email Analysis

- File Carving
- Email Header Analysis
- Determining File Headers
- Extraction of Attachments
- Extracting Specific File Types
- Deleted Files and Recovery

Module 6—Hash and Timeline Module

- Use of Hash Sets
- Adding Hash Sets
- Advantages of Timeline
- Timeline Creation

Module 7—Network-Based Monitoring

- Sources of Network Data
- PCAP Analysis with Wireshark
- Network Footprint

Recommended Pre-Work

Basic understanding of Unix, Windows OS, computer forensics, and TCP/IP networking is required for the course to be fully beneficial.

Module 8—Memory Forensics

- Basics of Memory Acquisition and Analysis
- Highlight Power of Memory

Module 9—Unix and Linux Incident Response

- Live Response Best Practices and Order of Volatility
- Following the Process Tree
- Unix/Linux File Permissions

Learn More

To order, or for further information, please call 1 888 847 8766 or email SecurityEducation@mcafee.com.

McAfee™
Together is power.

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com