

## Learning McAfee IntruShield Essentials

The McAfee IntruShield® course is an essential component of a successful intrusion prevention strategy. Hands-on labs show how to configure IntruShield to protect against real-world situations. This course puts knowledgeable administrators on the path to becoming intrusion prevention experts. The skills delivered in this course can be applied immediately, improving protection for your business and making certain that your investment in McAfee IntruShield realizes the utmost return.



### Skill Building

The following prerequisites are expected for successful completion of this course:

- Working knowledge of system administration concepts
- Basic understanding of computer security concepts

### Exercises

Topics are supported by hands-on exercises specifically designed to increase knowledge retention. Classroom exercises provide the basic hands-on experience needed to install, configure, and manage IntruShield sensors and Manager software.

### Course Materials

- Student Manual

### Duration

- Three Days

### Students Learn To

- Install, configure, and administer IntruShield sensors
- Install and configure IntruShield Manager
- Configure monitor ports
- Change from single port to port pair in-line mode
- Manage administrative domains, users, and roles
- Define and configure Alert viewer for historical attacks
- Define and configure Alert viewer in historical consolidated
- Drilldown into Alert viewer categories
- Enable and start incident generator service
- Describe how to generate the three categories of reports
- Manage policies with the policy editor
- Configure a VLAN or CIDR interface
- Define a reconnaissance policy
- Define a single Denial of Service (DoS) policy
- Describe administrative functions

### Suggested Next Course

To gain an enhanced set of skills and knowledge on host-based intrusion prevention and technologies:

- Learning McAfee Intercept Essentials (TRN-ENT-101-TCL)

### Contact Information

Phone: 866-210-2715

E-mail: [training@mcafee.com](mailto:training@mcafee.com)

Website: [www.mcafee.com](http://www.mcafee.com)

## Daily Outline

### Day 1

#### ***IntruShield Overview***

- Challenge with legacy IDS
- IntruShield sensor appliances
- IntruShield Security Management System
- IntruShield architecture
- IntruShield features and deployment flexibility
- Overview of intrusion prevention

#### ***IntruShield Sensor Overviews***

- I-1200, I-2600, I-4000
- Lab: Configure the sensor

#### ***IntruShield Manager Overview***

- Network console
- System health, configuration tool
- Alert viewer
- Report and incident generator
- Lab: Installing manager software
- Lab: Starting manager software

#### ***Update Server***

- Update options
- Update server authentication
- Updating policy and configuration
- Scheduled pushing

#### ***Sensor Deployment***

- Span or hub, TAP, and in-line modes
- Fail-open, fail-closed
- Fail-over pairing
- Port configuration
- Lab: Configuring monitor ports

### Day 2

#### ***Admin Domains***

- Logical overview
- Creating new admin domain and users
- Lab: Administrator domain nodes

#### ***Alert Viewer***

- Real-time vs. historical
- Viewer panels
- Drilldown views
- Acknowledging alerts
- Lab: Working with the Alert viewer

#### ***Incident Generation and Incident Viewer***

- Starting the generator service
- Configuring incident generator file
- Viewing incidents
- Viewer work overflow
- Lab: Enabling and starting incident generator service

#### ***Report Generator***

- IDS, configuration and scheduled reports
- Lab: Generating reports

#### ***Policies***

- IDS policy
- Attack categories
- Lab: Managing policies

### Day 3

#### ***Configuring Virtual IDS***

- Adding VLANs and child domains
- Defining CIDR interface
- Lab: Managing interfaces

#### ***Configuring DoS***

- DoS detection, profiles, and filters
- Policy inheritance
- Lab: Configuring DoS policies

#### ***Configuring User-Defined Signatures***

- UDS configuration and editor
- Creating a new signature

#### ***Configuring Checkpoint Firewall Responses***

- Creating OPSEC application entity
- Add OPSEC application to firewall
- Firewall filters

#### ***Configuring Failover***

- Creating failover pairs