

## Course 757

# Intrusion Detection Systems

### (3 days)

#### Course Description...

This course will examine the use of Intrusion Detection Systems (IDS) in an Enterprise network. Through real-world attacks against the classroom network, students will deploy and configure an IDS through a series of attack/response workshops. Once the IDS system has been configured, additional topics such as Network Vulnerability Scanning, Honeypots, and . To complete the course, the attendees will work in teams of two to four people on a case study to design and deploy an Intrusion Detection System for a multi-segment network, using the tools and techniques learned in the course. The Team and Case Study specifics can be customized to meet the specifics of the Enterprise.

#### Who Should Attend...

Attendees should include Managers, Network Security Officers, Network, System and Security Administrators, and Information Technology Personnel with a need to know how Intrusion Detection Systems can be utilized in an enterprise environment. Intrusion Detection Systems require extensive knowledge of TCP/IP, Networking, Firewalls, and System Administration – thus it is recommended that students have had training in these topics before attending this course.

#### Learning Objectives...

After completing this course, attendees will have an understanding of the capabilities of Intrusion Detection Systems, and the types of Intrusion Detection Systems available. Using this information, attendees will have the skills to assist their organization in evaluating and deploying open source and/or commercial Intrusion Detection Systems.

### Course Outline...

#### Overview – Intrusion Detection

- What is a Network Intrusion?
- What is Intrusion Detection?
- What is an Intrusion Detection System (IDS)?
- What are the costs associated with IDS?
- Commercial IDS Options
- Open-Source Options
- IDS Limitations: Excessive Monitoring and False Positives

#### Attacking a Network - Part 1

- Workshop: How to Attack a Network
- Network Monitoring
- Install and Configure a Simple IDS
- Using a Rules-based IDS
- Workshop: Detecting a Simple Network Attack



## **Attacking a Network - Part 2**

- Workshop: How to Attack a Network and avoiding Simple IDS
- When Network Monitoring and Simple IDS Fail
- Deploying IDS in switched and VLAN environments
- Locating IDS Sensors and Host-based IDS
- Workshop: Configure Advanced Capabilities of an IDS

## **Attacking a Network - Part 3**

- Workshop: Using a New Attack Vector to avoid Advanced IDS
- Understanding extensible IDS Systems
- Updating IDS Systems
- Writing a custom IDS Rule
- Workshop: Update IDS and create custom IDS rules

## **Reviewing Intrusion Detection System after an attack**

- Preserving IDS Configuration and Logs
- Legal Issues and IDS
- Reporting an Attack
- Responding to an Attack
- Re-playing an Attack

## **Supplementing/Enhancing an Intrusion Detection System**

- What is a Network Vulnerability Scanner?
- Overview of Open Source, Vendor Provided, and Commercial Vulnerability Scanners
- Workshop: Network Vulnerability Scanning
- What is a Honeypot?
- Determining appropriate use of a Honeypot
- Workshop: Building a honeypot on the network

## **Final Case Study: Prepare an Intrusion Detection System for a new network**

- ◆ **Teams of two to four attendees will build and deploy an IDS solution for a multi-segment network provided by the instructor.**

*Please contact your ROI representative to discuss course tailoring!!!*