Current Technologies
Computer Learning Centers

cisco Partner
Platinum Learning

Securing Cisco Networks with Open Source Snort (SSFSNORT) V4.0

WHERE GREAT TRAINING HAPPENS EVERYDAY!

Securing Cisco Networks with Open Source Snort (SSFSNORT) V4.0

Course Duration

4 Days

Course Price

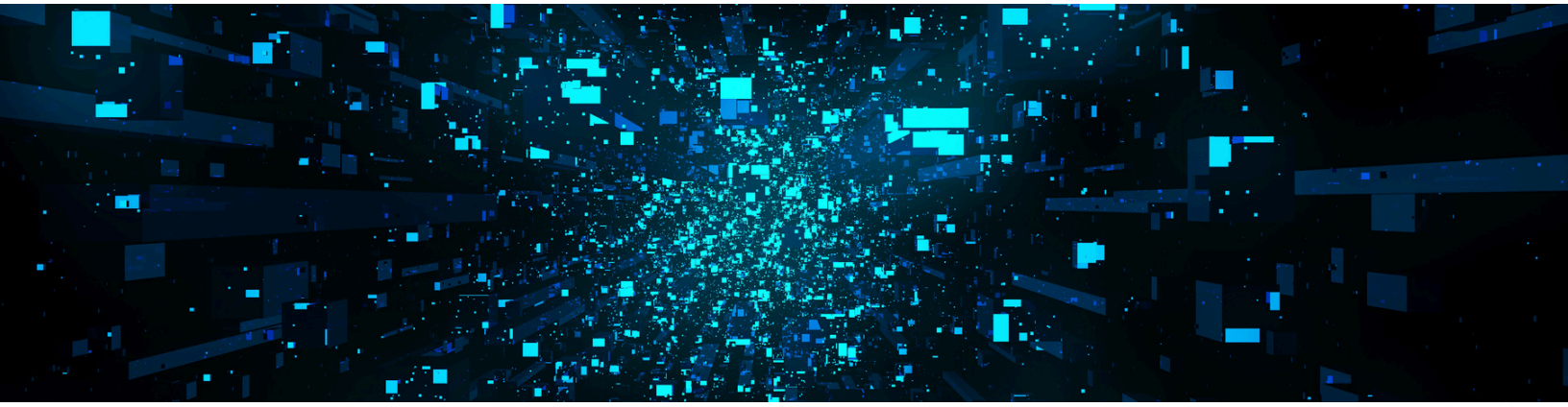
$3,595.00
36 CLCs

Methods of Delivery

In-Person ILT
Virtual ILT
Onsite ILT

About this Class

The Securing Cisco Networks with Open Source Snort (SSFSNORT) training shows you how to deploy a network intrusion detection system based on Snort. Through a combination of expert instruction and hands-on practice, you will learn how to install, configure, operate, and manage a Snort system. You will also explore rules writing with an overview of basic options, advanced rules writing, how to configure PulledPork, and how to use OpenAppID to provide protection of your network from malware. You will learn techniques of tuning and performance monitoring, traffic flow through Snort rules, and more. This training also earns you 32 Continuing Education (CE) credits toward recertification.



Securing Cisco Networks with Open Source Snort (SSFSNORT) V4.0

How you will benefit

This class will help you:

- Learn how to implement Snort, an open-source, rule-based, intrusion detection and prevention system
- Gain leading-edge skills for high-demand responsibilities focused on security
- Earn 32 CE credits towards recertification

Why Attend with Current Technologies CLC

- Our Instructors are the top 10% rated by Cisco
- Our Lab has a dedicated 1 Gig Fiber Connection for our Labs
- Our Labs run up to Date Code for all our courses

Who Should Attend

The job roles best suited to the material in this course are:

- Security Administrators
- Security Consultants
- Network Administrators
- System Engineers
- Technical Support Personnel
- Channel Partners and Resellers

Securing Cisco Networks with Open Source Snort (SSFSNORT) V4.0

Objectives

After taking this course, you should be able to:

- Describe Snort technology and identify the resources available for maintaining a Snort deployment
- Install and configure a Snort deployment
- Configure the command-line options for starting a Snort as a sniffer, a logger, and an intrusion detector, and create a script to start Snort automatically
- Identify and configure available Snort intrusion detection outputs
- Describe rule sources, updates, and utilities for managing rules and updates
- Detail the components of the snort.lua file and determine how to configure it for your deployment
- Configure Snort for inline operation using the inline-only features
- Configure rules for Snort using basic rule syntax
- Describe how traffic flows through Snort and how to optimize rules for better performance
- Configure advanced-rule options for Snort rules
- Configure OpenAppID features and functionality
- Tune Snort for efficient operation and profile system performance

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Securing Cisco Networks with Open Source Snort (SSFSNORT) V4.0

Course Outline

- **Module 1: Snort Technology Introduction**
- **Module 2: Snort Installation**
- **Module 3: Snort Operation Introduction**
- **Module 4: Snort Intrusion Detection Output**
- **Module 5: Rule Management**
- **Module 6: Snort Configuration**
- **Module 7: Inline Configuration and Operation**
- **Module 8: Snort Rule Syntax and Usage**
- **Module 9: Snort Rule Traffic Processing Flow**
- **Module 10: Advanced Rule Options**
- **Module 11: OpenAppID Detection Configuration**
- **Module 12: Snort Tuning**

+1 (219) 764-3800
6210 Central Ave, Portage IN
sales@ctclc.com
www.ctclc.com

Securing Cisco Networks with Open Source Snort (SSFSNORT) V4.0

Lab Outline

- Lab 1: Connecting to the Lab Environment
- Lab 2: Snort Installation
- Lab 3: Snort Operation
- Lab 4: Snort Intrusion Detection Output
- Lab 5: Pulled Pork Installation
- Lab 6: Configuring Variables
- Lab 7: Reviewing Preprocessor Configurations
- Lab 8: Inline Operations
- Lab 9: Basic Rule Syntax and Usage
- Lab 10: Advanced Rule Options
- Lab 11: OpenAppID Configuration
- Lab 12: Tuning Snort