# Securing Cisco Networks with Snort Rule Writing Best Practices (SSFRules)

## What you’ll learn in this course

The Securing Cisco Networks with Snort Rule Writing Best Practices (SSF Rules) v2.1 course shows you how to write rules for Snort, an open-source intrusion detection and prevention system. Through a combination of expert-instruction and hands-on practice, this course provides you with the knowledge and skills to develop and test custom rules, standard and advanced rules-writing techniques, how to integrate OpenAppID into rules, rules filtering, rules tuning, and more. The hands-on labs give you practice in creating and testing Snort rules.

## Course duration

- Instructor-led classroom: 3 days in the classroom with hands-on lab practice
- Instructor-led virtual classroom: 3 days of web-based classes with hands-on lab practice
- E-learning: Equivalent of 3 days of video-based instruction and practice

## How you’ll benefit

This course will help you:

- Gain an understanding of characteristics of a typical Snort rule development environment
- Gain hands-on practices on creating rules for Snort
- Gain knowledge in Snort rule development, Snort rule language, standard and advanced rule options

## Who should enroll

This course is for technical professionals to gain skills in writing rules for Snort-based Intrusion Detection Systems (IDS) and intrusion prevention systems (IPS). The primary audience includes:

- Security administrators
- Security consultants
- Network administrators
- System engineers
- Technical support personnel using open source IDS and IPS
- Channel partners and resellers

## Technology areas

- Security

## Course details

### Objectives

After taking this course, you should be able to:

- Describe the Snort rule development process
- Describe the Snort basic rule syntax and usage
- Describe how traffic is processed by Snort
- Describe several advanced rule options used by Snort
- Describe OpenAppID features and functionality
- Describe how to monitor the performance of Snort and how to tune rules

### Recommended knowledge and training

To fully benefit from this course, you should have:

- Basic understanding of networking and network protocols
- Basic knowledge of Linux command-line utilities
- Basic knowledge of text editing utilities commonly found in Linux
- Basic knowledge of network security concepts
- Basic knowledge of a Snort-based IDS/IPS system

## How to enroll

To enroll in the SSFRules course or explore our larger catalog of courses on Cisco Digital Learning, contact us at <training@fastlane-mea.com>

### Outline

- Introduction to Snort Rule Development
- Snort Rule Syntax and Usage
- Traffic Flow Through Snort Rules
- Advanced Rule Options
- OpenAppID Detection
- Tuning Snort

### Lab outline

- Connecting to the Lab Environment
- Introducing Snort Rule Development
- Basic Rule Syntax and Usage
- Advanced Rule Options
- OpenAppID
- Tuning Snort