# Securing Cisco Networks with Open Source Snort (SSFSNORT)

## Description

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 20 Continuing Education (CE) credits toward recertification.

## How you'll benefit

This training 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 20 CE credits toward recertification

## Who should enroll

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

## Technology areas

- Security
- Cyber Operations

## Objectives

- 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

## Prerequisites

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- Technical understanding of transmission control protocol/internet protocol (TCP/IP) networking and network architecture
- Proficiency with Linux and UNIX text editing tools, such as vi editor

These skills can be found in the following Cisco Learning Offering:

- Implementing and Administering Cisco Solutions (CCNA)

## Outline

- Snort Technology Introduction
- Snort Installation
- Snort Operation Introduction
- Snort Intrusion Detection Output
- Rule Management
- Snort Configuration
- Inline Configuration and Operation
- Snort Rule Syntax and Usage
- Snort Rule Traffic Processing Flow
- Advanced Rule Options
- OpenAppID Detection Configuration
- Snort Tuning

## Lab Outline

- Connecting to the Lab Environment
- Snort Installation

- Snort Operation
- Snort Intrusion Detection Output
- PulledPork Installation
- Configuring Variables
- Reviewing Preprocessor Configurations
- Inline Operation
- Basic Rule Syntax and Usage
- Advanced Rule Options
- OpenAppID Configuration
- Tuning Snort

## Links

- Cisco U. Learning Path
- Cisco Learning Network Store
- Cisco Learning Locator