**Document Generated: 11/14/2026**

**Learning Style: Virtual Classroom**

**Technology: Cisco**

**Difficulty: Intermediate**

**Course Duration: 4 Days**

# Securing Cisco Networks with Open Source Snort® v4.0 (SSFSNORT)



## About this course:

In this four-day course, Securing Cisco Networks with Open Source Snort®, students will learn how to build and manage a Snort® system using open source tools, plug-ins, as well as the Snort® rule language to help manage, tune, and deliver feedback on suspicious network activity.

This lab-intensive course introduces you to the open source Snort® technology, as well as rule writing. Among other powerful features, you become familiar with:

- How to build and manage a Snort® system
- How to update rules
- Snort® rules language
- The capabilities of Snort® when deployed passively and inline

The course begins by introducing the Snort® technology and progresses through the installation and operation of Snort®. You will discover the various output types that Snort® provides and learn about automated rule management including how to deploy and configure Pulled Pork, inline operations, and how to create custom Snort® rules, including advanced rule-writing techniques and OpenAppID.

This course combines lecture materials and hands-on labs that give you practice in deploying and managing Snort®.

## Course Objective:

Upon completing this course, the learner will be able to meet these overall objectives:

- Snort technology and identify the resources that are available for maintaining a Snort deployment
- Install Snort on a Linux-based operating system
- Snort operation modes and their command-line options
- Snort intrusion detection output options
- Download and deploy a new rule set to Snort
- Configure the snort.conf file
- Configure Snort for inline operation and configure the inline-only features
- Snort basic rule syntax and usage
- How traffic is processed by the Snort engine
- Several advanced rule options used by Snort
- OpenAppID features and functionality
- How to monitor of Snort performance and how to tune rules

## Audience:

The primary audience for this course is as follows:

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

## Prerequisite:

The knowledge and skills that the learner should have before attending this course are as follows:

- Networking and network protocols
- Linux command line utilities
- Text-editing utilities commonly found in Linux
- Network security concepts

## Course Outline:

**Introduction to Snort Technology**

**Snort Installation**

**Snort Operation**

**Snort Intrusion Detection Output**

**Rule Management**

**Snort Configuration**

**Inline Operation and Configuration**

**Snort Rule Syntax and Usage**

**Traffic Flow Through Snort Rules**

**Advanced Rule Options**

**OpenAppID Detection**

**Tuning Snort**

**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
- Lab 12: Tuning Snort

## Credly Badge:




**Display your Completion Badge And Get The Recognition You Deserve.**

Add a completion and readiness badge to your Linkedin profile, Facebook page, or Twitter account to validate your professional and technical expertise. With badges issued and validated by Credly, you can:

- Let anyone verify your completion and achievement by clicking on the badge
- Display your hard work and validate your expertise
- Display each badge's details about specific skills you developed.

Badges are issued by QuickStart and verified through Credly.

Find Out More or See List Of Badges