Document Generated: 09/11/2025

Learning Style: Virtual Classroom

Technology: Cisco

Difficulty: Intermediate

Course Duration: 4 Days

Securing Cisco Networks with Open Source SnortÂ® (SSFSNORT)

About this course:

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

deliver feedback on suspicious network activity.

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

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

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

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

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