

SSFSNORT

Securing Cisco Networks with Open Source Snort

The Securing Cisco Networks with Open Source Snort (SSFSNORT) course shows you how to set up 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 writing rules with an overview of basic options, writing advanced rules, configuring PulledPork, and using OpenAppID to protect your network from malware. You'll learn techniques for tuning and performance monitoring, traffic flow through Snort rules, and more.

Course Contents

- 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

E-Book You will receive the original course documentation from Cisco in English language as a Cisco E-Book. In the Cisco Digital Learning Version, the content of the courseware is integrated into the learning interface instead.

Target Group

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

Prerequisites

There are no prerequisites for this training course. However, it is recommended that you have the following knowledge and skills before attending this training course:

Course Target

This training will help you:

- Learn how to implement Snort, an open-source, rules-based intrusion detection and prevention system
- Acquire leading skills for demanding tasks in the field of security

Processing time

approx. 24 hours

This Course in the Web



You can find the up-to-date information and options for ordering under the following link:

www.expertech-training.com/go/CSFS

Reservation

On our Website, you can reserve a course seat for 7 days free of charge and in a non-committal manner. This can also be done by phone under +49 6074/4868-0.

Guaranteed Course Dates

To ensure reliable planning, we are continuously offering a wide range of guaranteed course dates.

Your Tailor-Made Course!

We can precisely customize this course to your project and the corresponding requirements.

Cisco Digital Learning

This course is available in the Cisco Digital Learning Library. These recently developed, multi-modal training events include HD videos moderated by lecturers with stored searchable text and subtitles, as well as exercises, labs, and explanatory text and graphics. We provide this offer to you via our myExpertech learning portal. Effective of the activation of the account, access to the courses will be granted for a duration of 6 months. In the case of packet solutions (Cisco Digital Learning Subscriptions), this time period will amount to 12 months.

Cisco Digital Learning	Prices, excl. of V.A.T.
	€ 500

Training	Prices, excl. of V.A.T.
Classes in Germany	4 Days € 3,995
Online Training	4 Days € 3,995
Date/course venue	Course language English
16/06-19/06/25	15/09-18/09/25
14/07-17/07/25	15/09-18/09/25
18/08-21/08/25	06/10-09/10/25
25/08-28/08/25	13/10-16/10/25

Status 05/14/2025



Table of Contents

SSFSNORT – Securing Cisco Networks with Open Source Snort

Course Outline

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

Labs Outline

This course contains 12 hands-on virtual lab exercises, powered by Cisco Learning Labs and Cisco IOL (Cisco IOS on Linux).



ExperTech Benelux B.V.

Ceresstraat 1 · 4811 CA Breda · Phone: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach-training.com