

Securing Cisco Networks with Open Source Snort (SSFSNORT)

ID SSFSNORT Price 3,995.— €(excl. tax) Duration 4 days

Course Overview

The Securing Cisco Networks with Open Source Snort (SSFSNORT) v2.1 course 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, rules writing with an overview of basic options, advanced rules writing, how to configure Pulled Pork, 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.

Who should attend

This course is for technical professionals who need to know how to deploy open source intrusion detection systems (IDS) and intrusion prevention systems (IPS), and how to write Snort rules.

- Security administrators
- Security consultants
- Network administrators
- System engineers
- Technical support personnel
- Channel partners and resellers

Prerequisites

To fully benefit from this course, you should have:

- Technical understanding of TCP/IP networking and network architecture
- Proficiency with Linux and UNIX text editing tools (vi editor is suggested by not required)

Course Objectives

After taking this course, you should be able to:

- Describe Snort technology and identify resources available for maintaining a Snort deployment

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

Course Benefits

This course 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

Detailed 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

- Connecting to the Lab Environment
- Snort Installation
- Snort Operation
- Snort Intrusion Detection Output

- Pulled Pork Installation
- Configuring Variables
- Reviewing Preprocessor Configurations
- Inline Operations
- Basic Rule Syntax and Usage
- Advanced Rule Options
- OpenAppID
- Tuning Snort

About Fast Lane



Fast Lane is a global, award-winning specialist in technology and business training as well as consulting services for digital transformation. As the only global partner of the three cloud hyperscalers- Microsoft, AWS and Google- and partner of 30 other leading IT vendors, Fast Lane offers qualification solutions and professional services that can be scaled as needed. More than 4,000 experienced Fast Lane professionals train and advise customers in organizations of all sizes in 90 countries worldwide in the areas of cloud, artificial intelligence, cyber security, software development, wireless and mobility, modern workplace, as well as management and leadership skills, IT and project management.

Fast Lane Services

- ✓ High End Technology Training
- ✓ Business & Soft Skill Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digital Learning Solutions
- ✓ Content Development
- ✓ Remote Labs
- ✓ Talent Programs
- ✓ Event Management Services

Training Methods

- ✓ Classroom Training
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Classroom & Online Hybrid
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobile Learning

Technologies & Solutions

- ✓ Digital Transformation
- ✓ Artificial Intelligence
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center



Worldwide Presence
with high-end training centers
around the globe



Multiple Awards
from vendors such as AWS,
Microsoft, Cisco, Google, NetApp,
VMware



Experienced SMEs
with over 19.000 combined
certifications

Germany

**Fast Lane Institute for Knowledge
Transfer GmbH**
Tel. +49 40 25334610
info@flane.de / www.flane.de

Austria

ITLS GmbH
(Partner of Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Switzerland

**Fast Lane Institute for Knowledge
Transfer (Switzerland) AG**
Tel. +41 44 8325080
info@flane.ch / www.flane.ch