

# Securing Cisco Networks with Snort Rule Writing Best Practices (SSFRULES)

**ID SSFRULES** Prix CHF 3 600,- (Hors Taxe) **Durée 3 jours**

## A qui s'adresse cette formation

This course is for technical professionals to gain skills in writing rules for Snort-based intrusion detection systems (IDS) and intrusion prevention systems (IPS). The primary audience includes:

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

## Pré-requis

To fully benefit from this course, you should have:

- Basic understanding of networking and network protocols
- Basic knowledge of Linux command-line utilities
- Basic knowledge of text editing utilities commonly found in Linux
- Basic knowledge of network security concepts
- Basic knowledge of a Snort-based IDS/IPS system

## Objectifs

After taking this course, you should be able to:

- Describe the Snort rule development process
- Describe the Snort basic rule syntax and usage
- Describe how traffic is processed by Snort
- Describe several advanced rule options used by Snort
- Describe OpenAppID features and functionality
- Describe how to monitor the performance of Snort and how to tune rules

## Centres de formation dans le monde entier



## Fast Lane Institute for Knowledge Transfer (Switzerland) AG

Husacherstrasse 3  
CH-8304 Wallisellen  
Tel. +41 44 832 50 80

info@flane.ch, <https://www.flane.ch>