

## Securing Cisco Networks with Open Source Snort

Durée: 4 Jours    Réf de cours: SSFSNORT    Version: 2.1

### Résumé:

The Securing Cisco Networks with Open Source Snort 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.

### Public visé:

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

### Objectifs pédagogiques:

- After completing this course, you should be able to:**
- Describe Snort technology and identify the resources that are 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 of Snort performance and how to tune rules

### Pré-requis:

#### Attendees should meet the following prerequisites:

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

### Test et certification

#### Recommended as preparation for exams:

- There are no exams currently aligned to this course

## Contenu:

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

## Autres moyens pédagogiques et de suivi:

- Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
- Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
- Modalités d'évaluation : le participant est invité à s'auto-évaluer par rapport aux objectifs énoncés.
- Chaque participant, à l'issue de la formation, répond à un questionnaire de satisfaction qui est ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

### Délais d'inscription :

- Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
- Votre place sera confirmée à la réception d'un devis ou "booking form" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
- Attention, si vous utilisez votre Compte Personnel de Formation pour financer votre inscription, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés.