# Securing Cisco Networks with Open Source Snort

**Duration: 4 Days** **Course Code: SSFSNORT** **Version: 3.0**

## Overview:

The Securing Cisco Networks with Open Source Snort course shows you how to deploy Snort® in small to enterprise-scale implementations. You will learn how to install, configure, and operate Snort in Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) modes. You'll practice installing and configuring Snort, utilize additional software tools and define rules to configure and improve the Snort environment, and more

## Target Audience:

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.

## Objectives:

- **After completing this course, you should be able to:**
- Define the use and placement IDS/IPS components.
- Identify Snort features and requirements.
- Compile and install Snort.
- Define and use different modes of Snort.
- Install and utilize Snort supporting software

## Prerequisites:

**Attendees should meet the following prerequisites:**

- Technical understanding of TCP/IP networking and network architecture
- Basic familiarity with firewall and IPS concepts

## Testing and Certification

**Recommended as preparation for exams:**

- There are no exams currently aligned to this course

## Content:

Detecting Intrusions with Snort 3.0

- History of Snort
- IDS
- IPS
- IDS vs. IPS
- Examining Attack Vectors
- Application vs. Service Recognition

Sniffing the Network

- Protocol Analyzers
- Configuring Global Preferences
- Capture and Display Filters
- Capturing Packets
- Decrypting Secure Sockets Layer (SSL) Encrypted Packets

Architecting Nextgen Detection

- Snort 3.0 Design
- Modular Design Support
- Plug Holes with Plugins
- Process Packets
- Detect Interesting Traffic with Rules
- Output Data

Choosing a Snort Platform

- Provisioning and Placing Snort
- Installing Snort on Linux

Operating Snort 3.0

- Topic 1: Start Snort
- Monitor the System for Intrusion Attempts
- Define Traffic to Monitor
- Log Intrusion Attempts
- Actions to Take When Snort Detects an Intrusion Attempt
- License Snort and Subscriptions

Examining Snort 3.0 Configuration

- Introducing Key Features
- Configure Sensors
- Lua Configuration Wizard

Managing Snort

- Pulled Pork
- Barnyard2
- Elasticsearch, Logstash, and Kibana (ELK)

Analyzing Rule Syntax and Usage

- Anatomy of Snort Rules
- Understand Rule Headers
- Apply Rule Options
- Shared Object Rules
- Optimize Rules
- Analyze Statistics

Use Distributed Snort 3.0

- Design a Distributed Snort System
- Sensor Placement
- Sensor Hardware Requirements
- Necessary Software
- Snort Configuration
- Monitor with Snort

Examining Lua

- Introduction to Lua
- Get Started with Lua

Labs

- Capture and Analyze Packets
- Initiate the Snort Installation
- Complete an Installation of Snort
- Configure and Run Snort
- Tweak the Installation
- Rapid Deployment with Lua
- Integrate Snort Optimizers
- Analyze Rule Syntax
- Hello World Lua Style

## Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK