Securing Cisco Networks with Open Source Snort®

Duración: 4 Días Código del Curso: SSFSNORT Version: 3.0 Método de Impartición: Curso Cerrado (In-Company)

Temario:

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.

e-Learning

Los servicios de e-learning y recursos on-demand que ofrece Global Knowledge, están diseñadas para permitir el acceso a los recursos de aprendizaje en cualquier lugar y en cualquier momento que convenga al alumno. Nuestra solución incluye la posibilidad de acceder a los equipos cuando se necesita para practicar sus habilidades y la oportunidad de ver y escuchar a nuestros expertos en la materia, ya que destacan las áreas clave de la formación.

Curso Cerrado (In-Company)

Debido a que nuestra formación es modular, nuestros responsables de formación e instructores pueden trabajar con usted y su equipo para detectar las necesidades formativas y adaptar un temario de forma rápida y rentable. Durante una formación cerrada, usted recibirá una formación de expertos en un curriculum adaptado a sus necesidades.

Dirigido a:

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.

Objetivos:

- **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

Prerequisitos:

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)

Exámenes y certificación

Recommended as preparation for exams:

- There are no exams currently aligned to this course

Contenido:

Module 1: Introduction to Snort Technology

Module 2: Snort Installation

Moudle 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

- Lab 1: Connecting to the Lab Environment
- 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

Más información:

Para más información o para reservar tu plaza llámanos al (34) 91 425 06 60

info.cursos@globalknowledge.es

www.globalknowledge.com/es-es/

Global Knowledge Network Spain, C/ Retama 7, 6ª planta, 28045 Madrid