kod szkolenia: SSFSNORT / PL AA 4d

Securing Cisco Networks with Open Source Snort

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. You'll 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.

Przeznaczenie szkolenia

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

Korzyści wynikające z ukończenia szkolenia

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

Oczekiwane przygotowanie słuchaczy

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)

Język szkolenia

- Szkolenie: polski
- Materiały: angielski

Czas trwania

4 dni / 28 godzin

Agenda szkolenia

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