Contact:
Info@silverlake.sg
+65 - 65882456

Securing Cisco Networks with Snort Rule Writing Best Practices

Course#:SSFRULES
Duration:3 Days
Price:0.00

Course Description

In this course, you will learn about the key features and characteristics of a typical Snort rule development environment. You will develop and test custom rules in a preinstalled Snort environment and identify how to use advanced rule-writing techniques. You will investigate how to include OpenAppID in your rules and also identify how to filter rules and monitor their performance.

This course combines lecture materials and hands-on labs that give you practice in creating Snort rules.

This lab-intensive course introduces you to Snort rule writing. Among other powerful features, you become familiar with:

- Snort rule development
- Snort rule language
- Standard and advanced rule options
- OpenAppID
- Tuning

Objectives

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

Audience

Security administrators
Security consultants
Network administrators
System engineers
Technical support personnel
Channel partners and resellers

Prerequisites

Basic understanding of:

Networking and network protocols
Linux command-line utilities
Text-editing utilities commonly found in Linux
Network security concepts
Snort-based IDS/IPS system

Content

Classroom Live Outline

Introduction to Snort Rule Development
Snort Rule Syntax and Usage
Traffic Flow Through Snort Rules
Advanced Rule Options
OpenAppID Detection
Tuning Snort

Classroom Live Labs

Lab 1: Connecting to the Lab Environment

Lab 2: Introducing Snort Rule Development

Lab 3: Basic Rule Syntax and Usage

Lab 4: Advanced Rule Options

Lab 5: OpenAppID

Lab 6: Tuning Snort