SSFRULES - SECURING CISCO NETWORKS WITH SNORT® RULE WRITING BEST PRACTICES V2.1

Course Code: 5827

Learn to analyze, exploit packet captures, and put the rule writing theories learned to work by implementing rule-language features for triggering alerts on the offending network traffic.

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

This course is eligible for 24 Continuing Education Credits (ILT & ELT Modality).

What You'll Learn

- 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

Who Needs to Attend

- 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

skillsoft global knowledge™

SSFRULES - SECURING CISCO NETWORKS WITH SNORT® RULE WRITING BEST PRACTICES V2.1

Course Code: 5827

CLASSROOM LIVE	$3,450 CAD	3 Day

Classroom Live Outline

1. Introduction to Snort Rule Development
2. Snort Rule Syntax and Usage
3. Traffic Flow Through Snort Rules
4. Advanced Rule Options
5. OpenAppID Detection
6. 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

SSFRULES - SECURING CISCO NETWORKS WITH SNORT® RULE WRITING BEST PRACTICES V2.1

Course Code: 5827

VIRTUAL CLASSROOM LIVE	$3,450 CAD	3 Day

Virtual Classroom Live Outline

1. Welcome to the Sourcefire Virtual Network
2. Basic Rule Syntax and Usage
3. Rule Optimization
4. Using PCRE in Rules
5. Using Byte_Jump/Test/Extract Rule Options
6. Protocol Modeling Concepts and Using Flowbits in Rule Writing
7. Case Studies in Rule Writing and Packet Analysis
8. Rule Performance Monitoring
9. Rule Writing Practical Labs, Exercises, and Challenges

Virtual Classroom Live Labs

- Lab 1: Writing Custom Rules
- Lab 2: Drop Rules
- Lab 3: Replacing Content
- Lab 4: SSH Rule Scenario
- Lab 5: Optimizing Rules
- Lab 6: Using PCREtest to Test Regex Options
- Lab 7: Use PCREtest to Test Custom Regular Expressions
- Lab 8: Writing Rules That Contain PCRE
- Lab 9: Detecting SADMIND Trust with Byte_Jump and Byte_Test
- Lab 10: Using the Bitwise AND Operation in Byte_Test Rule Option
- Lab 11: Detecting ZENworks Directory Traversal Using Byte_Extract
- Lab 12: Writing a Flowbit Rule
- Lab 13: Extra Flowbits Challenge

- Lab 14: Strengthen Your Brute-Force Rule with Flowbits
- Lab 15: Research and Packet Analysis
- Lab 16: Revisiting the Kaminsky Vulnerability
- Lab 17: Configuring Rule Profiling
- Lab 18: Testing Rule Performance
- Lab 19: Configure Rule Profiling to View PCRE Performance
- Lab 20: Preventing User Access to a Restricted Site
- Lab 21: SQL Injection
- Lab 22: The SQL Attack Revisited

Oct 27 - 29, 2025 | 9:00 AM - 5:00 PM EST

SSFRULES - SECURING CISCO NETWORKS WITH SNORT® RULE WRITING BEST PRACTICES V2.1

Course Code: 5827

ON-DEMAND	$1,300 CAD

On-Demand Outline

1. Introduction to Snort Rule Development
2. Snort Rule Syntax and Usage
3. Traffic Flow Through Snort Rules
4. Advanced Rule Options
5. OpenAppID Detection
6. Tuning Snort

On-Demand 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

Visit us at www.globalknowledge.com or call us at 1-866-716-6688.

Date created: 7/31/2025 2:08:39 AM