Securing Cisco Networks with Snort Rule Writing Best Practices (SSFSNORT)

Category: Networking & Security | **Vendor:** Cisco

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Course Overview

The Securing Cisco Networks with Snort Rule Writing Best Practices (SSFRules) v2.1 course shows you how to write rules for Snort, an open-source intrusion detection and prevention system. Through a combination of expert-instruction and hands-on practice, this course provides you with the knowledge and skills to develop and test custom rules, standard and advanced rules-writing techniques, how to integrate OpenAppID into rules, rules filtering, rules tuning, and more. The hands-on labs give you practice in creating and testing Snort rules.

This course will help you:

- Gain an understanding of characteristics of a typical Snort rule development environment
- Gain hands-on practices on creating rules for Snort
- Gain knowledge in Snort rule development, Snort rule language, standard and advanced rule options

About This Course

The Securing Cisco Networks with Snort Rule Writing Best Practices (SSFRules) v2.1 course shows you how to write rules for Snort, an open-source intrusion detection and prevention system. Through a combination of expert-instruction and hands-on practice, this course provides you with the knowledge and skills to develop and test custom rules, standard and advanced rules-writing techniques, how to integrate OpenAppID into rules, rules filtering, rules tuning, and more. The hands-on labs give you practice in creating and testing Snort rules.

This course will help you:

- Gain an understanding of characteristics of a typical Snort rule development environment
- Gain hands-on practices on creating rules for Snort
- Gain knowledge in Snort rule development, Snort rule language, standard and advanced rule options

Who Should Attend

This course is for technical professionals to gain skills in writing rules for Snort-based intrusion detection systems (IDS) and intrusion prevention systems (IPS). The primary audience includes:

- Security administrators
- Security consultants
- Network administrators
- System engineers
- Technical support personnel using open source IDS and IPS
- Channel partners and resellers

Prerequisites & Entry Requirements

General Prerequisites:

To fully benefit from this course, you should have:

- Basic understanding of networking and network protocols
- Basic knowledge of Linux command-line utilities
- Basic knowledge of text editing utilities commonly found in Linux
- Basic knowledge of network security concepts
- Basic knowledge of a Snort-based IDS/IPS system

Learning Outcomes

Upon successful completion of this course, participants will be able to:

After taking this course, you should be able to:

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

Detailed Course Outline

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

Skills You Will Learn:

After taking this course, you should be able to:

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

Frequently Asked Questions

Q: What delivery options are available for Securing Cisco Networks with Snort Rule Writing Best Practices (SSFSNORT)?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: How many CPD hours does this course provide?

The 3-day Securing Cisco Networks with Snort Rule Writing Best Practices (SSFSNORT) course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Securing Cisco Networks with Snort Rule Writing Best Practices (SSFSNORT) training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Securing Cisco Networks with Snort Rule Writing Best Practices (SSFSNORT)?

Yes, we provide corporate training, dedicated training, and closed classes for Securing Cisco Networks with Snort Rule Writing Best Practices (SSFSNORT). Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Securing Cisco Networks with Snort Rule Writing Best Practices, Intrusion Prevention, AMP, Firewall, VPN, SSFRULES

Q: Why choose Nexus Human for Securing Cisco Networks with Snort Rule Writing Best Practices (SSFSNORT)?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Securing Cisco Networks with Snort Rule Writing Best Practices (SSFSNORT) training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)