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

COURSE OVERVIEW:

The Securing Cisco Networks with Snort Rule Writing Best Practices (SSFRules) v2.0 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 the 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 WILL BENEFIT FROM THIS COURSE?

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

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

COURSE OBJECTIVES:

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

COURSE OUTLINE:

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

SUNSET LEARNING INSTITUTE (SLI) DIFFERENTIATORS:

Sunset Learning Institute (SLI) has been an innovative leader in developing and delivering authorized technical training since 1996. Our goal is to help our customers optimize their cloud technology investments by providing convenient, high quality technical training that our customers can rely on. We empower students to master their desired technologies for their unique environments.

What sets SLI apart is not only our immense selection of trainings options, but our convenient and consistent delivery system. No matter how complex your environment is or where you are located, SLI is sure to have a training solution that you can count on!

Premiere World Class Instruction Team

- All SLI instructors have a four-year technical degree, instructor level certifications and field consulting work experience.
- Sunset Learning has won numerous Instructor Excellence and Instructor Quality Distinction awards since 2012

Enhanced Learning Experience

- The goal of our instructors during class is ensure students understand the material, guide them through our labs and encourage questions and interactive discussions.

Convenient and Reliable Training Experience

- You have the option to attend classes at any of our established training facilities or from the convenience of your home or office with the use of our HD-ILT network (High Definition Instructor Led Training)
- All Sunset Learning Institute classes are guaranteed to run – you can count on us to deliver the training you need when you need it!

Outstanding Customer Service

- Dedicated account manager to suggest the optimal learning path for you and your team
- Enthusiastic Student Services team available to answer any questions and ensure a quality training experience