Securing Cisco Networks with Open Source Snort v3.0 (SSFSNORT)

Price: 3600

Duration: 4 days

Delivery Methods: Virtual

Overview

Securing Cisco Networks with Open Source Snort (SSFSNORT) v3.0 is a 4-day course that shows you how to deploy Snort® in small to enterprise-scale implementations. You will learn how to install, configure, and operate Snort in Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) modes. You'll practice installing and configuring Snort, utilize additional software tools and define rules to configure and improve the Snort environment, and more.

This course will help you:

- Learning 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.

Prerequisites:

The knowledge and skills that the learner should have before attending this course are as follows:

- Technical understanding of TCP/IP networking and network architecture
- Basic familiarity with firewall and IPS concepts

This is the recommended Cisco course that may help you meet these prerequisites:

- Implementing and Administering Cisco Solutions (CCNA)

Course Objectives:

Upon completing this course, the learner will be able to meet these overall objectives:

- Define the use and placement IDS/IPS components.
- Identify Snort features and requirements.
- Compile and install Snort.
- Define and use different modes of Snort.
- Install and utilize Snort supporting software.

Who Should Attend

The primary audience for this course is as follows:

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

Course content

Module 1: Detecting Intrusions with Snort 3.0

- History of Snort
- IDS
- IPS
- IDS vs. IPS
- Examining Attack Vectors
- Application vs. Service Recognition

Module 2: Sniffing the Network

- Protocol Analyzers
- Configuring Global Preferences
- Capture and Display Filters
- Capturing Packets
- Decrypting Secure Sockets Layer (SSL) Encrypted Packets

Module 3: Architecting Nextgen Detection

- Snort 3.0 Design
- Modular Design Support
- Plug Holes with Plugins
- Process Packets
- Detect Interesting Traffic with Rules
- Output Data

Module 4: Choosing a Snort Platform

- Provisioning and Placing Snort
- Installing Snort on Linux

Module 5: Operating Snort 3.0

- Start Snort
- Monitor the System for Intrusion Attempts
- Define Traffic to Monitor
- Log Intrusion Attempts
- Actions to Take When Snort Detects an Intrusion Attempt
- License Snort and Subscriptions

Module 6: Examining Snort 3.0 Configuration

- Introducing Key Features
- Configure Sensors
- Lua Configuration Wizard

Module 7: Managing Snort

- Pulled Pork
- Barnyard2
- Elasticsearch, Logstash, and Kibana (ELK)

Module 8: Analyzing Rule Syntax and Usage

- Anatomy of Snort Rules
- Understand Rule Headers
- Apply Rule Options
- Shared Object Rules
- Optimize Rules

- Analyze Statistics

Module 9: Use Distributed Snort 3.0

- Design a Distributed Snort System
- Sensor Placement
- Sensor Hardware Requirements
- Necessary Software
- Snort Configuration
- Monitor with Snort

Module 10: Examining Lua

- Introduction to Lua
- Get Started with Lua

Course Schedule

Date	Time	Price	Options

Why Professional Choose TOPTALENT?

Dedicated Texas-Based Support

Get assistance every step of the way from our **Texas-based team**, ensuring your training experience is hassle-free and aligned with your goals.

3000+ Curated Professional Courses

Access an extensive portfolio of over 3000 courses across IT, Business Application and Leadership – Designed to meet evolving Industry demands

95% Client Approval Rating

Trusted by professionals nationwide our 95% approval rating reflects consistent quality, measurable impact and exceptional service.

Certified Industry Instructor

Learn from professionaly certified experts with real world experience and a proven commitment to learner success.

For questions

call:

(469) 721-6100

Email:

info@toptalentlearning.com

Find More Training

FAQ

What if I have to reschedule my class due to conflict?

Ten (10) business days' notice is required to reschedule a class with no additional fees. Notify TOPTALENT LEARNING as soon as possible at 469-721-6100 or by written notification to info@toptalentlearning.com to avoid rescheduling penalties.

How do I enroll for this class?

Please contact our team at 469-721-6100; we will gladly guide you through the online purchasing process.

What happens once I purchase a class?

You will receive a receipt and an enrollment confirmation sent to the email you submitted at purchase. Your enrollment email will have instructions on how to access the class. Any additional questions our team is here to support you. Please call us at 469-721-6100.

What is your late policy?

If a student is 15 minutes late, they risk losing their seat to a standby student. If a student is 30 minutes late or more, they will need to reschedule. A no-show fee will apply. Retakes are enrolled on a stand-by basis. The student must supply previously issued courseware. Additional fees may apply.

What happens when I finish my class?

You will receive a ‘Certificate of Completion’ once you complete the class. If you purchased an exam voucher for the class, a team member from TOPTALENT LEARNING will reach out to discuss your readiness for the voucher and make arrangements to send it.