

SSFSNORT

Securing Cisco Networks with Open Source Snort

Die Schulung Securing Cisco Networks with Open Source Snort (SSFSNORT) zeigt Ihnen, wie Sie ein auf Snort basierendes Network Intrusion Detection System einrichten. Durch eine Kombination aus fachkundiger Anleitung und praktischer Übung lernen Sie, wie Sie ein Snort-System installieren, konfigurieren, betreiben und verwalten. Sie werden auch das Schreiben von Regeln mit einem Überblick über grundlegende Optionen, das Schreiben von Regeln für Fortgeschrittene, die Konfiguration von PulledPork und die Verwendung von OpenAppID zum Schutz Ihres Netzwerks vor Malware erkunden. Sie lernen Techniken zur Abstimmung und Leistungsüberwachung, den Traffic-Fluss durch Snort-Regeln und vieles mehr.

Kursinhalt

- Describe Snort technology and identify the resources available for maintaining a Snort deployment
- Install and configure a Snort deployment
- Configure the command-line options for starting a Snort as a sniffer, a logger, and an intrusion detector, and create a script to start Snort automatically
- Identify and configure available Snort intrusion detection outputs
- Describe rule sources, updates, and utilities for managing rules and updates
- Detail the components of the snort.lua file and determine how to configure it for your deployment
- Configure Snort for inline operation using the inline-only features
- Configure rules for Snort using basic rule syntax
- Describe how traffic flows through Snort and how to optimize rules for better performance
- Configure advanced-rule options for Snort rules
- Configure OpenAppID features and functionality
- Tune Snort for efficient operation and profile system performance

E-Book Sie erhalten die englischen Original-Unterlagen als Cisco E-Book. Bei der Cisco Digital Learning Version sind die Inhalte der Kursunterlagen stattdessen in die Lernoberfläche integriert.

Zielgruppe

- Security Administrators
- Security Consultants
- Network Administrators
- System Engineers
- Technical Support Personnel
- Channel Partners and Resellers

Voraussetzungen

Für diese Schulung gibt es keine Voraussetzungen. Es wird jedoch empfohlen, dass Sie vor der Teilnahme an dieser Schulung folgende Kenntnisse und Fähigkeiten besitzen:

- Technisches Verständnis des Transmission Control Protocol/Internet Protocol (TCP/IP) und der Netzwerkarchitektur
- Kenntnisse im Umgang mit Linux- und UNIX-Textverarbeitungsprogrammen, z. B. vi-Editor

Diese Kenntnisse finden Sie im folgenden Kurs von Cisco:

- Implementing and Administering Cisco Solutions (CCNA)

Kursziel

Diese Schulung wird Ihnen helfen:

- Sie lernen, wie Sie Snort, ein regelbasiertes Open-Source-System zur Erkennung und Verhinderung von Eindringlingen, implementieren.
- Erwerben Sie führende Fähigkeiten für anspruchsvolle Aufgaben im Bereich der Sicherheit

Bearbeitungszeit

ca. 24 Stunden

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.at/go/CSFS

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Cisco Digital Learning & Cisco U.

Die multimodalen Schulungen der Cisco Digital Learning Library beinhalten referenzgeführte HD-Videos mit hinterlegtem durchsuchbarem Text und Untertiteln, Übungen, Labs und erklärenden Text sowie Grafiken. Das Angebot stellen wir Ihnen über unser Lernportal myExperTeach zur Verfügung. Der Zugriff auf die Kurse steht ab der Freischaltung für einen Zeitraum von sechs Monaten zur Verfügung. Bei Paketen (Cisco U.) beträgt dieser Zeitraum zwölf Monate.

Cisco Digital Learning & Cisco U. Preise zzgl. MwSt.
6 Monate Freischaltung € 500,-

Training		Preise zzgl. MwSt.
Termine in Österreich	4 Tage	€ 3.995,-
Online Training	4 Tage	€ 3.995,-
Termin/Kursort	Kursprache Englisch 	
16.06.-19.06.25 	15.09.-18.09.25 	
14.07.-17.07.25 	15.09.-18.09.25 	
18.08.-21.08.25 	06.10.-09.10.25 	
25.08.-28.08.25 	13.10.-16.10.25 	

Stand 14.05.2025



Inhaltsverzeichnis

SSFSNORT – Securing Cisco Networks with Open Source Snort

Course Outline

- Snort Technology Introduction
- Snort Installation
- Snort Operation Introduction
- Snort Intrusion Detection Output
- Rule Management
- Snort Configuration
- Inline Configuration and Operation
- Snort Rule Syntax and Usage
- Snort Rule Traffic Processing Flow
- Advanced Rule Options
- OpenAppID Detection Configuration
- Snort Tuning

Lab Outline

- Connecting to the Lab Environment
- Snort Installation
- Snort Operation
- Snort Intrusion Detection Output
- PulledPork Installation
- Configuring Variables
- Reviewing Preprocessor Configurations
- Inline Operation
- Basic Rule Syntax and Usage
- Advanced Rule Options
- OpenAppID Configuration
- Tuning Snort

