

SSFSNORT

Securing Cisco Networks with Open Source Snort

Der Cisco Training on Demand-Kurs **Securing Cisco Networks with Open Source Snort (SSFSNORT) Version 2.0** bietet Ihnen eine technische Schulung für den erfolgreichen Einsatz der **Open-Source-Snort-Technologie** und das Schreiben von Regeln. Neben anderen leistungsstarken Funktionen lernen Sie, wie Sie ein **Snort-System aufbauen und verwalten** und wie Sie Regeln effizient aktualisieren und verwalten können. Sie lernen auch die **Snort-Regelsprache** und die Fähigkeiten von **Snort** kennen, wenn es **passiv und inline** eingesetzt wird. Darüber hinaus lernen Sie die **Voraussetzungen für die Installation, die korrekte Konfiguration und den Betrieb** von Snort kennen. Sie erwerben Kenntnisse über die **Geschichte, die Funktionen und die Einsatzmöglichkeiten** von Snort sowie über die **öffentlichen Ressourcen, die Snort-Benutzern zur Verfügung stehen**. Schließlich lernen Sie die **verschiedenen Ausgabetypen, die Snort bereitstellt, die automatische Regelverwaltung (einschließlich der Bereitstellung und Konfiguration von Pulled Pork), Inline-Operationen und die Erstellung benutzerdefinierter Snort-Regeln, einschließlich fortgeschrittener Regelschreibtechniken und OpenAppID.**

Kursinhalt

- Describe Snort technology and identify the resources that are available for maintaining a Snort deployment
- Install Snort on a Linux - based operating system
- Describe the Snort operation modes and their command - line options
- Describe the Snort intrusion detection output options
- Download and deploy a new rule set to Snort
- Describe and configure the snort.conf file
- Configure Snort for inline operation and configure the inline - only features
- Describe the Snort basic rule syntax and usage
- Describe how the Snort engine processes traffic
- Describe several advanced rule options used by Snort
- Describe OpenAppID features and functionality
- Describe how to monitor Snort performance and how to tune rules

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

Zielgruppe

This course is designed for security administrators and consultants, network administrators, systems engineers, and technical support personnel who need to know how to deploy open-source intrusion detection systems (IDS) and intrusion prevention systems (IPS), and how to write Snort rules.

Voraussetzungen

Die für die Teilnahme an diesem Kurs erforderlichen Kenntnisse und Fähigkeiten sind:

- Grundlegendes Verständnis von Netzwerken und Netzwerkprotokollen
- Grundlegende Kenntnisse der Linux-Befehlszeilen- und Textverarbeitungsprogramme, die in Linux üblich sind
- Grundkenntnisse von Netzwerksicherheitskonzepten

Bearbeitungszeit

ca. 24 Stunden

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.expertech.ch/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 myExpertech 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 **CHF 550,-**

Training Preise zzgl. MwSt.

Termine in der Schweiz 4 Tage

Online Training 4 Tage CHF 4.395,-

Termin/Kursort Kurssprache Englisch

13.05.-16.05.24 Online 01.07.-04.07.24 Online

17.06.-20.06.24 Online



Inhaltsverzeichnis

SSFSNORT – Securing Cisco Networks with Open Source Snort

Course Outline

Module 1: Introduction to Snort Technology
Module 2: Snort Installation
Module 3: Snort Operation
Module 4: Snort Intrusion Detection Output
Module 5: Rule Management
Module 6: Snort Configuration
Module 7: Inline Operation and Configuration
Module 8: Snort Rule Syntax and Usage
Module 9: Traffic Flow Through Snort Rules
Module 10: Advanced Rule Options
Module 11: OpenAppID Detection
Module 12: Tuning Snort

Labs Outline

This course contains 12 hands-on virtual lab exercises, powered by Cisco Learning Labs and Cisco IOL (Cisco IOS on Linux).



ExperTeach AG

Kronenstrasse 11 · 8735 St. Gallenkappel · Telefon: +41 55 420 2591 · Fax: +41 55 420 2592 · info@experteach.ch · www.experteach.ch