

# IPS v7

## Implementing Cisco Intrusion Prevention System



Mit den Sensoren der 4200er Serie sowie dem Intrusion Detection Service Module 2 (IDSM-2) der Catalyst 6000er Serie stehen leistungsfähige Komponenten zur Verfügung, um ein Intrusion Detection and Prevention System aufzusetzen. Der Kurs vermittelt mittels vieler praktischer Übungen alle dafür erforderlichen Fertigkeiten. Im Fokus steht der IPS Device Manager (IDM), der für Konfiguration und Management der Cisco IPS Sensor Platform sowie zur Ansicht und zur Reaktion auf IPS Sensor Alarms verwendet wird. Die Inhalte dieses Kurses bereiten auf den Test 642-627 (IPS) vor, der Teil der Zertifizierung zum CCNP Security sowie für die Zertifizierung zum Cisco IPS Specialist erforderlich ist.

### Kursinhalt

- Intrusion Prevention und Security Policies
- Installation und Inbetriebnahme einer Sensor Appliance
- Installation und Initialisierung eines IDSM-2 in einem Cisco Catalyst 6500
- IDS Command Line Interface
- Umgang mit dem IPS Device Manager (IDM)
- Signatur- und Service Pack Updates
- Upgrade und Recovery des Sensor Images, automatische Software Upgrades
- Backup und Restore der Sensoren mit dem CLI
- Monitoring der Sensoren mit CLI und IDM
- Grundkonfiguration der Sensoren
- User Accounts
- Signature Engines und ihre Parameter
- Der Software Bypass Mode
- Konfiguration von Signaturen
- Optimieren der Sensor-Einstellungen
- Blocking Configuration
- Alarm Monitoring und Management
- Troubleshooting-Kommandos
- IPS Manager Express
- Global Correlation

Jeder Teilnehmer erhält die englischsprachigen Original-Unterlagen von Cisco.

### Zielgruppe

Der Kurs eignet sich für Techniker und Administratoren, die mit Cisco Komponenten ein Intrusion Prevention System konfigurieren und betreiben wollen.

### Voraussetzungen

Neben Netzwerkgrundlagen werden gute Kenntnisse von Ethernet und TCP/IP erwartet. Im Umgang mit dem Cisco IOS müssen Sie sattelfest sein – das Wissen eines CCNA wird vorausgesetzt.



### Vormerkung und Buchung

Gerne merken wir für Sie für die Dauer von zwei Wochen kostenfrei und unverbindlich einen Kursplatz vor. Auf [www.expertech.de](http://www.expertech.de) können Sie unter *Anmeldung* bequem Vormerkung, Buchung und Hotelreservierung vornehmen. Oder rufen Sie uns einfach an unter 06074-4868-0.

Für geschlossene Teilnehmergruppen modifizieren wir diesen Kursinhalt gerne entsprechend Ihren Anforderungen. Bitte sprechen Sie uns an!



Auf Wunsch senden wir Ihnen gerne unseren kompletten Katalog zu, der Sie über alle Trainings und andere Dienstleistungen informiert.

**5 Tage €2.590,00 • CHF 4.295,00 • zzgl. MwSt.**

#### Termin/Kursort

18.06.-22.06.12	Berlin	05.11.-09.11.12	Düsseldorf
18.06.-22.06.12	Hamburg	26.11.-30.11.12	Berlin
09.07.-13.07.12	München	26.11.-30.11.12	Hamburg
09.07.-13.07.12	Wien	17.12.-21.12.12	Stuttgart
23.07.-27.07.12	Frankfurt	17.12.-21.12.12	Wien
23.07.-27.07.12	Zürich	17.12.-21.12.12	München
13.08.-17.08.12	Düsseldorf	28.01.-01.02.13	Frankfurt
03.09.-07.09.12	Berlin	28.01.-01.02.13	Zürich
03.09.-07.09.12	Hamburg	11.02.-15.02.13	Düsseldorf
08.10.-12.10.12	München	04.03.-08.03.13	Hamburg
08.10.-12.10.12	Wien	04.03.-08.03.13	Berlin
22.10.-26.10.12	Frankfurt		

Aktuelle Informationen finden Sie auf [www.expertech.de](http://www.expertech.de) IPS7

IPS v7



EXPERTeCh



Security & WLAN

IT & TK Training

- 1. Introduction to Intrusion Prevention and Detection, Cisco IPS Software, and Supporting Devices**
  - 1.1. Evaluating Intrusion Prevention and Intrusion Detection Systems
  - 1.2. Choosing Cisco IPS Software, Hardware, and Supporting Applications
  - 1.3. Evaluating Network IPS Traffic Analysis Methods, Evasion Possibilities, and Anti-
  - 1.4. Choosing a Network IPS and IDS Deployment Architecture
  
- 2. Installing and Maintaining Cisco IPS Sensors**
  - 2.1. Integrating the Cisco IPS Sensor into a Network
  - 2.2. Performing the Cisco IPS Sensor Initial Setup
  - 2.3. Managing Cisco IPS Devices
  
- 3. Applying Cisco IPS Security Policies**
  - 3.1. Configuring Basic Traffic Analysis
  - 3.2. Implementing Cisco IPS Signatures and Responses
  - 3.3. Configuring Cisco IPS Signature Engines and the Signature Database
  - 3.4. Deploying Anomaly-Based Operation
  
- 4. Adapting Traffic Analysis and Response to the Environment**
  - 4.1. Customizing Traffic Analysis
  - 4.2. Managing False Positives and False Negatives
  - 4.3. Improving Alarm and Response Quality
  
- 5. Managing and Analyzing Events**
  - 5.1. Installing and Integrating Cisco IPS Manager Express with Cisco IPS Sensors
  - 5.2. Managing and Investigating Events Using Cisco IPS Manager Express
  - 5.3. Using Cisco IME Reporting and Notifications
  - 5.4. Integrating Cisco IPS with Cisco Security Manager and Cisco Security MARS
  - 5.5. Using the Cisco IntelliShield Database and Services
  
- 6. Deploying Virtualization, High Availability, and High Performance Solutions**
  - 6.1. Using Cisco IPS Virtual Sensors
  - 6.2. Deploying Cisco IPS for High Availability and High Performance
  
- 7. Configuring and Maintaining Specific Cisco IPS Hardware**
  - 7.1. Configuring and Maintaining the Cisco ASA AIP-SSM and AIP-SSC-5 Modules
  - 7.2. Configuring and Maintaining the Cisco ISR IPS AIM and IPS NME Modules
  - 7.3. Configuring and Maintaining the Cisco IDSM-2



**ExperTeach Gesellschaft für Netzwerkkompetenz mbH**

Waldstr. 94 • D-63128 Dietzenbach

Telefon +49 6074 4868-0 • Telefax +49 6074 4868-109

info@experteach.de • www.experteach.de

© ExperTeach GmbH, alle Angaben ohne Gewähr

Stand 12.05.2012