

# Trend Micro Deep Security 20 Training for Certified Professionals

Trend Micro™ Deep Security Training für Certified Professionals ist ein Kurs, in dem die Teilnehmer lernen, wie Trend Micro™ Deep Security für die Einrichtung einer Advanced Hybrid-Cloud Security auf physischen, virtuellen und Cloud-basierten Computern eingesetzt wird. Der Kurs beschreibt die Grundarchitektur der Deep Security-Lösung, Bereitstellungsoptionen, Protection-Module, Policy-Konfigurationen und Administration des Systems. Im Rahmen des Kurses werden Deep Security Agents auf einer Reihe von Windows® Server-Plattformen sowie die Deep Security Virtual Appliance eingesetzt. Weiterhin werden Best Practices und Details des Troubleshooting für eine erfolgreiche Implementierung und eine langfristige Wartung des Systems diskutiert. Der Kurs zeigt ebenfalls die in Trend Micro Cloud One™ verfügbaren Services und die XDR-Funktionen von Trend Micro Vision One™. Am Ende des Kurses wird die lokale Installation der Deep Security Software auf Trend Micro Cloud One™ - Workload Security migriert. Das theoretische Wissen wird in zahlreichen Übungen in die Praxis umgesetzt.

Nach Abschluss des Kurses können die Teilnehmer die Zertifizierungsprüfung zum Trend Micro Certified Professional for Deep Security ablegen. Die Prüfung ist im Kurspreis inkludiert.

#### Kursinhalt

- Product Overview
- Trend Micro™ Deep Security™ Manager
- Deploying Deep Security Agents
- Managing Deep Security Agents
- Keeping Deep Security Up to Date
- Trend Micro™ Smart Protection™
- Policies
- Protecting Servers from Malware
- Blocking Malicious Websites
- Filtering Traffic Using the Firewall
- Protecting Servers from Vulnerabilities
- Detecting Changes to Protected Servers
- Blocking Unapproved Software
- Inspecting Logs on Protected Servers
- Events and Alerts
- Automating Deep Security Operations
- Detecting Emerging Malware Through Threat Intelligence
- Integrating with Trend Micro Vision One
- Migrating to Cloud One – Workload Security
- Appendix Topics

**E-Book** Sie erhalten ausführliche Kursunterlagen von Trend Micro in englischer Sprache. Wahlweise stellen wir die Printversion oder ein Trend Micro e-Kit zur Verfügung.

#### Zielgruppe

Dieser Kurs richtet sich an IT-Experten, die für den Schutz von Usern, Netzwerken, Rechenzentren und Cloud-Ressourcen vor Datenmissbrauch und gezielten Angriffen verantwortlich sind.

Dazu gehören auch die Verantwortlichen für:

- Operations
- Deployment
- Security Response
- Compliance
- Support

#### Voraussetzungen

Praktische Erfahrungen im Umgang mit den Trend Micro Produkten sowie grundlegende Netzwerkkennnisse sind hilfreich. Ebenso Kenntnisse im Umgang mit folgenden Produkten: Windows Servers und Clients, Firewalls, Packet Inspection Devices, VMware ESXi/vCenter/NSX, Amazon Web Services/Microsoft® Azure®/VMware vCloud®/Google Cloud Platform™, Virtualisierungstechnologien.

#### Kursziel

Nach Abschluss des Kurses können die Teilnehmer die Zertifizierungsprüfung zum Trend Micro Certified Professional for Deep Security ablegen. Die Prüfung ist im Kurspreis inkludiert. Für die Registrierung zum Examen wird ein Account im Trend Micro Education Portal benötigt.

#### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.ch/go/TMDS](http://www.experteach.ch/go/TMDS)

#### 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.

Training	Preise zzgl. MwSt.
<b>Termine in Deutschland</b>	<b>3 Tage CHF 2.195,-</b>
<b>Termine in Österreich</b>	<b>3 Tage CHF 2.195,-</b>
<b>Termine in der Schweiz</b>	<b>3 Tage CHF 2.795,-</b>
<b>Online Training</b>	<b>3 Tage CHF 2.195,-</b>
<b>Termin/Kursort</b>	Kurssprache Deutsch 
09.10.-11.10.24  Online	05.02.-07.02.25  Online
13.11.-15.11.24 Zürich	08.04.-10.04.25  Online
09.12.-11.12.24  Frankfurt	08.04.-10.04.25  Wien
09.12.-11.12.24  Online	11.06.-13.06.25  Frankfurt
05.02.-07.02.25  München	11.06.-13.06.25  Online

Stand 20.09.2024



# Inhaltsverzeichnis

## Trend Micro Deep Security 20 Training for Certified Professionals

### Product Overview

- Introduction to Deep Security
- Deep Security protection modules
- Deep Security deployment options
- Deep Security components

### Trend Micro™ Deep Security™ Manager

- Server, operating system, and database requirements
- Deep Security Manager architecture
- Installing and upgrading Deep Security Manager

### Deploying Deep Security Agents

- Deep Security agent architecture
- Deploying Deep Security agents

### Managing Deep Security Agents

- Command line operations
- Resetting agents
- Protecting agents
- Viewing computer protection status
- Upgrading Deep Security agents
- Organizing computers using groups and Smart Folders

### Keeping Deep Security Up to Date

- Security updates
- Software updates
- Deep Security relays

### Trend Micro™ Smart Protection™

- Smart Protection services used by Deep Security
- Configuring the Smart Protection source

### Policies

- Policy inheritance and overrides
- Creating new policies
- Running recommendation scans

### Protecting Servers from Malware

- Anti-malware scanning techniques
- Enabling anti-malware protection
- Smart Scan

### Blocking Malicious Websites

- Enabling web reputation

- Setting the security level

### Filtering Traffic Using the Firewall

- Enabling the Deep Security firewall
- Firewall rules
- Traffic analysis
- Traffic order of analysis
- Port scan

### Protecting Servers from Vulnerabilities

- Virtual patching
- Detecting suspicious network activity
- Web application protection
- Enabling intrusion prevention
- Intrusion prevention rules
- Security Sockets Layer (SSL) filtering
- Protecting web applications

### Detecting Changes to Protected Servers

- Enabling integrity monitoring
- Running recommendation scans
- Detection changes to baseline objects

### Blocking Unapproved Software

- Enforcement modes
- Enabling application control
- Detecting software changes
- Creating an inventory of approved software
- Pre-approving software changes

### Inspecting Logs on Protected Servers

- Enabling log inspection
- Running recommendation scans

### Events and Alerts

- Event forwarding
- Alerts
- Event tagging
- Reporting

### Protecting Containers

- Continuous integration/continuous deployment
- Software development using containers
- Protecting containers with Deep Security

### Automating Deep Security Operations

- Scheduled tasks
- Event-based tasks
- Quick start templates
- Baking the Deep Security agent into an Amazon® Machine Image
- Application programming interface

### Detecting Emerging Malware Through Connected Threat Defense

- Connected Threat Defense phases
- Trend Micro™ Deep Discovery™ Analyzer
- Trend Micro Apex Central™
- Configuring Deep Security for Connected Threat Defense
- Tracking submissions

### Appendix Topics

- Activating and managing multiple tenants
- Protecting virtual machines using the Deep Security virtual appliance
- Troubleshooting common Deep Security issues

