

Trend Micro Apex One for Certified Professionals

In this course, you will learn how to use Trend Micro Apex One™. This course details basic architecture, protection functionality, deployment scenarios, and troubleshooting. Through hands-on labs, participants practice configuring Apex One protection features, along with the administration options needed for a successful implementation and longterm maintenance. Taught by Trend Micro certified trainers, this course incorporates a variety of hands-on lab exercises, allowing participants to put the lesson content into action.

Kursinhalt

- Apex One Overview
- Apex One Server
- Apex One Web Management Console
- Security Agents
- Managing Off-Premise Agents
- Keeping Apex One Updated
- Trend Micro Smart Protection
- Protecting Endpoint Computers from Malware
- Protecting Endpoint Computers Through Behavior Monitoring
- Protecting Endpoint Computers from Unknown Threats
- Detecting Emerging Malware Through Trend Micro™ Connected Threat Defense
- Blocking Web Threats
- Protecting Endpoint Computers Through Traffic Filtering
- Preventing Data Leaks on Endpoint Computers
- Deploying Policies Through Apex Central
- Blocking Unapproved Applications on Endpoint Computers
- Protecting Endpoint Computers from Vulnerabilities
- Detecting and Investigating Security Incidents on Endpoint Computers
- Troubleshooting Apex One

E-Book Jeder Teilnehmer erhält ausführliche Kursunterlagen von Trend Micro in englischer Sprache. Wahlweise stellen wir die Printversion oder ein Trend Micro e-Kit zur Verfügung.

Zielgruppe

This course is designed for IT professionals responsible for protecting endpoint computers from data breaches and targeted attacks.

This includes those involved with:

- Operations
- Deployment
- Security Response
- Compliance

Voraussetzungen

There are no prerequisites to attend this course, however, a working knowledge of Trend Micro products and services, as well as an understanding of basic networking concepts and principles will be helpful.

Basic knowledge of the following topics is also beneficial:

- Windows® servers and clients
- Microsoft® Internet Information Server (IIS)
- General understanding of malware

Kursziel

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

Stand 14.05.2019

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.expertech.de/go/TMAP

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.	
Classroom Training	3 Tage	€ 1.995,-
Termin/Kursort		
02.07.-04.07.19	Zürich	26.11.-28.11.19 Zürich
13.08.-15.08.19	Frankfurt	14.01.-16.01.20 Wien
10.09.-12.09.19	Lausanne	11.02.-13.02.20 Frankfurt
30.09.-02.10.19	München	09.03.-11.03.20 München
22.10.-24.10.19	Hamburg	



Inhaltsverzeichnis

Trend Micro Apex One for Certified Professionals

Apex One Overview

- Trend Micro solutions
- Key features of Apex One
- Apex One components
- Deployment methods
- Threat detection

Apex One Server

- Apex One Server tasks
- Apex One Server services and components
- Configuration repositories
- Installing/upgrading Apex One Server
- Apex One plug-ins and utilities

Apex One Web Management Console

- Logging into the console
- Integrating with Active Directory
- Creating new administrative accounts

Security Agents

- Security Agent tasks
- Security Agent services and components
- Security Agent tree
- Installing Agents
- Migrating from other endpoint security software
- Agent-to-Server/Server-to-Agent communication
- Endpoint location
- Moving Security Agents
- Uninstalling Security Agents
- Agent settings and grouping
- Agent self-protection
- Agent privileges

Managing Off-Premise Agents

- Protection features
- Installing the Apex One Edge Relay Server
- Registering the Apex One Edge Relay Server
- Edge Relay Server and external Agent communication
- Edge Relay Server digital certificates

Keeping Apex One Updated

- ActiveUpdate
- Updating the Apex One Server
- Updating Security Agents
- Update Agents

- Security compliance

Trend Micro Smart Protection

- Smart Protection services and sources
- Configuring the Smart Protection source

Protecting Endpoint Computers from Malware

- Scanning for malware
- Scan settings
- Quarantining malware
- Smart Scan
- Spyware/grayware protection
- Preventing outbreaks

Protecting Endpoint Computers Through Behavior Monitoring

- Malware behavior blocking
- Ransomware protection
- Anti-exploit protection
- Fileless malware protection
- Newly encountered program detection
- Event monitoring
- Behavior monitoring exceptions

Protecting Endpoint Computers from Unknown Threats

- Common Vulnerabilities and Exposures exploits
- Predictive machine learning
- Offline predictive machine learning

Detecting Emerging Malware Through Trend Micro™ Connected Threat Defense

- Connected Threat Defense requirements
- Deep Discovery Analyzer
- Suspicious Objects

Blocking Web Threats

- Web reputation
- Detecting suspicious connections
- Protecting against browser exploits

Protecting Endpoint Computers Through Traffic Filtering

- Firewall filtering
- Application filtering
- Certified Safe Software list

- Stateful inspection
- Intrusion Detection System
- Firewall policies and profiles

Preventing Data Leaks on Endpoint Computers

- Data Loss protection
- Installing Data Loss protection
- Configuring data identifiers, data loss prevention templates and policies
- Device control

Deploying Policies Through Apex Central

- Apex Central
- Apex Central management modes
- Managing Apex One policies in Apex Central
- Data Discovery policies

Blocking Unapproved Applications on Endpoint Computers

- Integrated Application Control
- Application Control criteria
- Implementing Application Control
- User-based Application Control
- Lockdown Mode
- Best practices

Protecting Endpoint Computers from Vulnerabilities

- Integrated Vulnerability Protection
- Vulnerability Protection Pattern
- Implementing Vulnerability Protection
- Network Engine settings

Detecting and Investigating Security Incidents on Endpoint Computers

- Integrated Endpoint Sensor
- Endpoint Detection and Response
- Apex One Incident Response Model
- Managed Detection and Response

Troubleshooting Apex One

- Debugging the Apex One Server and Agents
- Troubleshooting communication issues
- Troubleshooting virus infection
- Troubleshooting Apex One services
- Troubleshooting sample submission



ExperTeach GmbH

Waldstraße 94 • 63128 Dietzenbach • Telefon: +49 6074 4868-0 • Fax: +49 6074 4868-109
info@experitech.de • www.experitech.de

