

Trend Micro Deep Security 11.x for Certified Professionals

Trend Micro™ Deep Security 11.0 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. Als Teil des Kurses werden die Teilnehmer Deep Security in einer virtuellen Umgebung installieren, Agent-Endpoint-Computer einrichten und den Schutz dieser Computer konfigurieren. Weiterhin werden Best Practices und Details des Troubleshootings für eine erfolgreiche Implementierung und eine langfristige Wartung des Systems diskutiert. Der Kurs basiert auf Deep Security 11.0. 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 Deep Security** ablegen. Die Prüfung ist im Kurspreis inkludiert.

Kursinhalt

- Lösungsüberblick und -Architektur
- Deep Security Manager
- Deep Security Agent
- Installation, Deployment und Konfiguration der verschiedenen Module
- Integration mit VMware Technologien
- Agent-based und Agent-less Szenarien
- Performance und Sizing des Produkts
- Deployment Szenarien
- Security in Cloud-Szenarien

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

Dieser Kurs ist für IT-Profis, die für die IT-Sicherheit und den Schutz von IT-Infrastrukturen insbesondere in Data Centern und Cloud-Umgebungen verantwortlich sind: System Administrators, Network Engineers, Support Engineers, Integration Engineers, Solution & Security Architects.

Voraussetzungen

Praktische Erfahrungen im Umgang mit den Trend Micro Produkten sowie grundlegende Netzwerkkennnisse werden vorausgesetzt. Außerdem sollten Sie Erfahrung im Umgang mit folgenden Produkten haben: Windows Servers und Clients, Firewalls, Packet Inspection Devices, VMware ESXi/vCenter/NSX, Amazon AWS/Microsoft Azure/VMware vCloud, Virtualisierungstechniken und -technologien.

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.de/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. | |
|---------------------------|---------------|----------------------|-----------|
| Classroom Training | 3 Tage | € 1.895,- | |
| Termin/Kursort | | Kurssprache Deutsch | |
| 17.06.-19.06.19 | Wien | 10.12.-12.12.19 | Zürich |
| 16.07.-18.07.19 | Zürich | 28.01.-30.01.20 | Wien |
| 27.08.-29.08.19 | Frankfurt | 25.02.-27.02.20 | Frankfurt |
| 14.10.-16.10.19 | München | 23.03.-25.03.20 | München |
| 12.11.-14.11.19 | Hamburg | | |
| Termin/Kursort | | Kurssprache Englisch | |
| 24.09.-26.09.19 | Lausanne | | |

Stand 26.05.2019



Inhaltsverzeichnis

Trend Micro Deep Security 11.x for Certified Professionals

Product Overview

- Trend Micro solutions
- Introduction to Deep Security
- Deep Security Protection Modules
- Deep Security components

Deep Security Manager

- Server and operating system requirements
- Database requirements
- Deep Security Manager architecture and components
- Automating tasks
- Installing Deep Security Manager
- Upgrading Deep Security Manager
- Logging into the Deep Security Manager Web console

Deep Security Agent

- Deep Security Agent architecture
- Installing Deep Security Agents
- Adding computers
- Activating Deep Security Agents
- Upgrading Deep Security Agents to Relays
- Distributing software and security updates
- Viewing computer protection status
- Organizing computers using Groups and Smart Folders

Policies

- Policy inheritance and overrides
- Creating policies based on Recommendation Scans
- Creating new policies
- Common objects

Protecting Servers From Malware

- Enabling Anti-Malware protection
- Anti-Malware scanning techniques
- Viewing Anti-Malware-related events
- Reviewing identified files
- Smart Scan

Blocking Malicious Web Sites

- Enabling Web Reputation
- Setting the security level
- Viewing Web Reputation-related events

Filtering Traffic Using Firewall Rules

- Enabling the Deep Security Firewall
- Firewall Rules

- Traffic Analysis
- Rule order of analysis
- Stateful and pseudo-stateful filtering
- Port scanning
- Viewing Firewall-related events

Protecting Servers From Vulnerabilities

- Virtual Patching
- Protocol Hygiene
- Protocol Control
- Web Application Protection
- Enabling Intrusion Prevention
- Running Recommendation Scans
- Intrusion Prevention rules
- SSL filtering
- Protecting Web applications

Detecting Changes to Protected Servers

- Enabling Integrity Monitoring
- Running Recommendation Scans
- Detection changes to the baseline object
- Event tagging
- Viewing Integrity Monitoring-related events

Blocking Unapproved Software

- Enforcement Modes
- Enabling Application Control
- Detecting software changes
- Creating an inventory of approved software
- Viewing Application Control-related events

Inspecting Logs on Protected Servers

- Enabling Log Inspection
- Running Recommendation Scans
- Viewing Log Inspection-related events

Logging and Reports

- Enabling diagnostic logging
- Creating diagnostic packages
- Event forwarding
- Reporting
- Filtering report data

Activating and Managing Multiple Tenants

- Enabling Multi-Tenancy
- Creating tenants

- Managing tenants
- Activating Deep Security Agents on tenants
- Usage monitoring

Detecting Emerging Malware Through Connected Threat Defense

- Connected Threat Defense requirements
- Deep Discovery Analyzer
- Trend Micro Control Manager
- Integrating Deep Security into Connected Threat Defense

Protecting Virtual Machines Using the Deep Security Virtual Appliance

- Agentless protection
- Deploying Deep Security in VMWare ESXi environments
- Configuring Affinity settings



ExperTeach GmbH

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

