



Trend Micro™ Deep Security Training for Certified Professionals

Course Description:

In this course, you will learn how to use Trend Micro™ Deep Security. This course provides information about the basic architecture, deployment scenarios, installation processes, policy configuration and administration options, as well as troubleshooting details that a network administrator needs to know for successful implementation and long-term maintenance.

Target Audience:

This course is designed for IT professionals who are responsible for protecting networks from any kind of networked, endpoint, or cloud security threats.

The individuals who will typically benefit the most include:

- System administrators
- Network engineers
- Support Engineers
- Integration Engineers
- Solution & Security Architects

Course Prerequisites:

Before you take this course, Trend Micro recommends that you have a working knowledge of their products and services, as well as basic networking concepts and principles.

You should also have a working knowledge or understanding of the following:

- Windows servers and clients
- Firewalls, WAFs, Packet Inspection devices
- Microsoft Internet Information Server (IIS), Apache
- VMware ESXi / vCenter / vShield
- Amazon AWS / Microsoft Azure / VMware vCloud
- Virtualisation techniques and technologies

Course Topics:

- Overview
 - Key Functionality
 - Components and Architecture
- Installation Planning and Deployment
- Product In-Depth
 - Deep Security Manager and Agent
 - Update and Software Management
 - Integration
- Endpoint Management
 - Detection Methods and Agent Activation
 - Deep Security Relays
 - Security Updates
- Policy Management
 - Inheritance, Hierarchy, and Overrides
 - Common Objects
- Anti-Malware Solution Platform (AMSP)
 - Anti-Malware Scan Engines
 - Scans and Quarantine
 - Smart Protection
- Web Reputation
 - Security Levels and Exceptions
 - Web Reputation Communication
 - Analysis Process
- Firewall
 - Firewall Rules
 - Reconnaissance Scans
 - Traffic Analysis
- Intrusion Prevention
 - Virtual Patching
 - Protocol Hygiene
 - Application Control
 - Web Application Protection
 - Recommendation Scans
- Integrity Monitoring
 - Event Tagging
- Log Inspection
- Logging and Reports
- Multi-Tenancy
- Agentless Protection
- Cloud Computing
 - Amazon AWS, Microsoft Azure and VMware vCloud