Trend Micro™ Deep Security 12 Training for Certified Professionals Course Outline

Authorized Training Center

Length	**3 Day**
Courseware	**eBooks**

Course Description

Trend Micro™ Deep Security 12 Training for Certified Professionals is a three-day, instructor-led training course where participants will learn how to use Trend Micro™ Deep Security for advanced server security of physical, virtual and cloud-based computers. This course details the basic architecture of the Deep Security solution, deployment options, protection modules, policy configuration, and administration of the system. As part of the course, participants will install Deep Security Manager in a virtual lab environment, deploy Deep Security Agents on endpoint computers, and configure protection on these computers. Best practices and troubleshooting details for successful implementation and long-term maintenance of the system are also discussed. This course is based on Deep Security 10, Feature Release 3.

This course incorporates a variety of hands-on lab exercises allowing participants to put the lesson content into action.

This course is taught by Trend Micro-certified trainers. Upon completion of this course, participants may complete the certification examination to obtain designation as a Trend Micro Certified Professional for Deep Security.

Target Audience

This course is designed for IT professionals who are responsible for protecting users, networks, data centres and cloud resources from data breaches and targeted attacks.

This includes those responsible for:

- Operations
- Deployment
- Security Response
- Compliance
- Support

CERTIFICATIONS AND RELATED EXAMINATIONS:

Upon completion of this course, participants may choose to complete the certification exam to obtain designation as a **Trend Micro Certified Professional for Deep Security**.

Prerequisites

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

- Firewalls and packet inspection devices
- VMware ESXi / vCenter / NSX
- Amazon AWS / Microsoft Azure / VMware vCloud
- Virtualization technologies

Participants are required to bring a laptop computer with a screen resolution of at least 1980 x 1080 or above; a display size of 15" or above is recommended.

Course Topics

Course topics are divided into the following lessons.

Product Overview

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

Deep Security Manager

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

Deep Security Agents

- Deep Security Agent architecture
- Deploying Deep Security 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

Protecting Servers from Malware

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

Blocking Malicious Websites

- Enabling web reputation
- Setting the security lev

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
- Protocol hygiene
- Protocol control
- Web application protection
- Enabling intrusion prevention
- Running recommendation scans
- 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

Activating and Managing Multiple Tenants

- Segmentation using multi-tenancy
- Enabling multi-tenancy
- Creating and managing tenants
- Activating Deep Security Agents on tenants
- Usage monitoring

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 submission

Protecting Virtual Machines Using the Deep Security Virtual Appliance

- Deep Security Virtual Appliance
- Virtual Appliance deployment models
- Virtual appliance deployment and activation