

Trend Micro

DEEP SECURITY TRAINING FOR CERTIFIED PROFESSIONALS

In this course, participants will learn how to use Trend Micro Deep Security for advanced hybrid cloud security on physical, virtual, and cloud-based servers. 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 a variety of Windows® server computers, and configure protection. Best practices and troubleshooting details for successful implementation and long-term maintenance of the system are also discussed.

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.

COURSE OBJECTIVES:

The course topics in this training are divided into the following lessons:

- Describe the purpose, features, functions, and capabilities of Trend Micro Deep Security 11.0
- Define and install components that make up Deep Security
- Implement security by enabling protection modules
- Review available configuration and administration options
- Attempt the Trend Micro Certified Professional for Deep Security Certification Exam

WHY CHOOSE VERACOMP EDUCATION

- Hands-on instruction and best practice advice from our experienced trainers
- With Trend Micro product certifications, you have the skills to deploy and manage their leading security solutions
- By sharpening your skills, you are more able to detect and respond to the latest attacks

Target Audience:

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

This includes those involved with:

- Operations
- Deployment
- Security Response
- Compliance

Available courses from Trend Micro's official curriculum:

- Trend Micro Certified Professional for Apex One
- Trend Micro Certified Professional for Deep Security
- Trend Micro Certified Professional for Deep Discovery

Training

Price: 950 EUR

* 3 days course, materials and certification included, lunch and refreshments provided

Need customized course?

No problem! We can deliver course according to your preferred topic, course location or length.

DETAILED COURSE OUTLINE:

Topics covered:

Product Overview

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

Deep Security Manager

- Server, operating system, and database requirements
- Deep Security Manager components
- Automating tasks
- Installing or upgrading Deep Security Manager

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 new policies

Protecting Servers from Malware

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

Blocking Malicious Web Sites

- Enabling web reputation
- Setting the security level

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

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 the baseline object
- Event tagging

Blocking Unapproved Software

- Enforcement modes
- Enabling Application Control
- Detecting software changes
- Creating an inventory of approved software

Inspecting Logs on Protected Servers

- Enabling log inspection
- Running recommendation scans

Logging and Reports

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

Activating and Managing Multiple Tenants

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

Protecting Virtual Machines using the Deep Security Virtual Appliance

- Agentless protection
- Deploying Deep Security in VMWare ESXi environments