Authorized Training Center

Trend Micro™ DEEP SECURITY 20 TRAINING FOR CERTIFIED PROFESSIONALS

Course Title: Trend Micro Deep Security 20 Training for Certified Professionals
Course Length: Three Days
Level: Professional
Delivery Language: English

Course Description

Trend Micro Deep Security Software 20 Training for Certified Professionals is a three-day, instructor-led training course. Participants will learn how to use Deep Security Software for advanced hybrid cloud security on physical, virtual, and cloud-based servers. This course details the basic architecture of the on-premises Deep Security Software solution, deployment options, protection modules, policy configuration, and administration of the system. As part of the course, participants will deploy Deep Security Software agents on a variety of Windows Server platforms. Best practices and troubleshooting details for successful implementation and long-term maintenance of the system are discussed. Participants will also be introduced to the XDR and threat intelligence capabilities of Trend Vision One™.

This course is taught by Trend Micro certified trainers and incorporates a variety of hands-on lab exercises, allowing participants to put the lesson content into action.

Target audience and Course Prerequisites

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 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 software.**

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 Web Services/Microsoft® Azure®/VMware vCloud®/Google Cloud Platform™

- Virtualization technologies

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

Course Objectives:

After completing this training course, participants will be able to:

- Describe the purpose, features, functions, and capabilities of Deep Security 20

- Define and install components that make up Deep Security

- Implement security by enabling protection modules

- Integrate Deep Security software with Trend Micro XDR

- Attempt the Trend Micro Certified Professional for Deep Security Certification exam

Detailed course outline:

Topics covered:

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

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

Deploying Deep Security Agents
- Deep Security agent architecture
- Deploying Deep Security agents

Managing Deep Security Agents
- Command line operations
- Resetting agents
- Protecting agents
- Viewing computer protection status
- Upgrading Deep Security agents
- Organizing computers using groups and Smart Folders
- Protecting container hosts

Keeping Deep Security Up to Date
- Security updates
- Software updates
- Deep Security relays

Global Threat Intelligence
- Global threat intelligence services used by Deep Security Software
- Configuring the global threat intelligence source

Policies
- Policy inheritance and overrides
- Creating new policies
- Running recommendation scans

Protecting Servers from Malware
- Anti-malware scanning techniques
- Enabling anti-malware protection
- Trend Micro™ Smart Scan™

Blocking Malicious Websites
- Enabling web reputation
- Setting the security level

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
- Detecting suspicious network activity
- Protocol control
- Web application protection
- Enabling intrusion prevention
- 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

Controlling Access to External Storage Devices
- Enforcement settings
- Enabling device control

Events and Alerts
- Event forwarding
- Alerts
- Event tagging

- Reporting

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

Integrating with Trend Vision One
- Trend Vision One capabilites
- Collecting telemetry
- Connecting Deep Security Software to Trend Vision One
- Endpoint inventory
- Trend Endpoint Basecamp

Introduction to XDR Threat Investigation
- Detection models
- Observed attack techniques
- Navigating within workbenches
- Searching within the data lake

Detecting Emerging Malware Through Threat Intelligence
- Threat Intelligence phases
- Threat Intelligence requirements
- Configuring Deep Security Software for Threat Intelligence
- Tracking submissions

Appendix Topics
- Activating and managing multiple tenants
- Troubleshooting common Deep Security issues