Trend Micro Certified Professional Deep Security

Category: Networking & Security | **Vendor:** Trend Micro

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format: Instructor Led - Online

Certification: Certified Professional for Deep Security

Course Overview

Trend Micro™ Deep Security™ 20 Training for Certified Professionals is a three-day, instructor-led training course.

Participants will learn how to use Trend Micro™ Deep Security™ software for advanced hybrid cloud security on physical, virtual, and cloudbased servers. This course details the basic architecture of the on-premises Deep Security solution, deployment options, protection modules, policy configuration, and administration of the system. As part of the course, participants will deploy Deep Security agents on a variety of Windows® Server platforms, as well as the Deep Security Virtual Appliance. Best practices and troubleshooting details for successful implementation and long-term maintenance of the system are discussed.

About This Course

Course Topics

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

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 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
- 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
- Certification
- Trend Micro Certified Professional for Deep Security Certification Exam

Prerequisites & Entry Requirements

General 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 recommended screen resolution of at least 1980 x 1080 or above and a display size of 15” or above.

Learning Outcomes

Upon successful completion of this course, participants will be able to:

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

- Describe the purpose, features, functions, and capabilities of Trend Micro Deep Security 12
- Define and install components that make up Deep Security Implement security by enabling protection modules
- Describe available configuration and administration options
- Attempt the Trend Micro Certified Professional for Deep Security Certification Exam.
- 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.

Detailed Course Outline

Course Topics

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

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 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

- 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
- Certification
- Trend Micro Certified Professional for Deep Security Certification Exam

Skills You Will Learn:

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

- Describe the purpose, features, functions, and capabilities of Trend Micro Deep Security 12
- Define and install components that make up Deep Security Implement security by enabling protection modules
- Describe available configuration and administration options
- Attempt the Trend Micro Certified Professional for Deep Security Certification Exam.
- 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.

Frequently Asked Questions

Q: What delivery options are available for Trend Micro Certified Professional Deep Security?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The Trend Micro Certified Professional Deep Security course helps prepare you for the Certified Professional for Deep Security certification path.

Q: How many CPD hours does this course provide?

The 3-day Trend Micro Certified Professional Deep Security course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Trend Micro Certified Professional Deep Security training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Trend Micro Certified Professional Deep Security?

Yes, we provide corporate training, dedicated training, and closed classes for Trend Micro Certified Professional Deep Security. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Trend Micro Certified Professional Deep Security, Trend Micro, CPDS

Q: Why choose Nexus Human for Trend Micro Certified Professional Deep Security?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Trend Micro Certified Professional Deep Security training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)