Deep Security Training for Certified Professionals

Duration: 3 Days **Course Code: TMDS**

Overview:

Trend Micro™ Deep Security™ 12 Training for Certified Professionals is a three-day, instructor-led training 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 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.
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 centers, and cloud resources from data breaches and targeted attacks.
This includes those responsible for:
Operations
Deployment
Security Response
Compliance
Support

Objectives:

- 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

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 andprinciples 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.

Content:

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™ :

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

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

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

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

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

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo