



Trend Micro Apex One Training for Certified Professionals

Duration: 3 Days **Course Code: TMAO**

Overview:

In this course, you will learn how to use Trend Micro Apex One™. This course details basic architecture, protection functionality, deployment scenarios, and troubleshooting.

Through hands-on labs, participants practice configuring Apex One protection features, along with the administration options needed for a successful implementation and longterm maintenance.

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

Target Audience:

This course is designed for IT professionals responsible for protecting endpoint computers from data breaches and targeted attacks. This includes those involved with:

- Operations
 - Deployment
 - Security Response
 - Compliance
-

Objectives:

- After completing this course, participants will be able to:
 - Describe the purpose, features, functions, and capabilities of Apex One
 - Define the components that make up Apex One
 - Implement security using Security Agents
 - Configure and administer Apex One Servers and Agents
 - Deploy Apex One policies using Trend Micro Apex Central
 - Troubleshoot common issues
 - Attempt the Trend Micro Certified Professional for Apex One 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

and principles will be helpful.

Basic knowledge of the following topics is also beneficial:

Windows® servers and clients

Microsoft® Internet Information Server (IIS)

General understanding of malware

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.

Testing and Certification

-

Content:

Apex One Overview	Updating Security Agents	Stateful inspection
Trend Micro solutions	Update Agents	Intrusion Detection System
Key features of Apex One	Security compliance	Firewall policies and profiles
Apex One components	Trend Micro Smart Protection :	Preventing Data Leaks on Endpoint Computers
Deployment methods	Smart Protection services and sources	Data Loss protection
Threat detection	Configuring the Smart Protection source	Installing Data Loss protection
Apex One Server	Protecting Endpoint Computers from Malware	Configuring data identifiers, data loss prevention templates and policies
Apex One Server tasks	Scanning for malware	Device control
Apex One Server services and components	Scan settings	Deploying Policies Through Apex Central
Configuration repositories	Quarantining malware	Apex Central
Installing/upgrading Apex One Server	Smart Scan	Apex Central management modes
Apex One plug-ins and utilities	Spyware/grayware protection	Managing Apex One policies in Apex Central
Apex One Web Management Console	Preventing outbreaks	Data Discovery policies
Logging into the console	Protecting Endpoint Computers Through Behavior Monitoring:	Blocking Unapproved Applications on Endpoint Computers:
Integrating with Active Directory	Malware behavior blocking	Integrated Application Control
Creating new administrative accounts	Ransomware protection	Application Control criteria
Security Agents	Anti-exploit protection	Implementing Application Control
Security Agent tasks	Fileless malware protection	User-based Application Control
Security Agent services and components	Newly encountered program detection	Lockdown Mode
Security Agent tree	Event monitoring	Best practices
Installing Agents	Behavior monitoring exceptions	

Migrating from other endpoint security software	Protecting Endpoint Computers from Unknown Threats :	Protecting Endpoint Computers from Vulnerabilities:
Agent-to-Server/Server-to-Agent communication	Common Vulnerabilities and Exposures exploits	Integrated Vulnerability Protection
Endpoint location	Predictive machine learning	Vulnerability Protection Pattern
Moving Security Agents	Offline predictive machine learning	Implementing Vulnerability Protection
Uninstalling Security Agents	Detecting Emerging Malware Through Trend	Network Engine settings
Agent settings and grouping	Connected Threat Defense requirements	Detecting and Investigating Security Incidents on Endpoint Computers
Agent self-protection	Deep Discovery Analyzer	Integrated Endpoint Sensor
Agent privileges	Suspicious Objects	Endpoint Detection and Response
Managing Off-Premise Agents	Blocking Web Threats:	Apex One Incident Response Model
Protection features	Web reputation	Managed Detection and Response
Installing the Apex One Edge Relay Server	Detecting suspicious connections	Troubleshooting sample submission Apex One
Registering the Apex One Edge Relay Server	Protecting against browser exploits	Debugging the Apex One Server and Agents
Edge Relay Server and external Agent communication	Protecting Endpoint Computers Through :	Troubleshooting communication issues
Edge Relay Server digital certificates	Traffic Filtering	Troubleshooting virus infection
Keeping Apex One Updated	Firewall filtering	Troubleshooting Apex One services
ActiveUpdate	Application filtering	Troubleshooting sample submission
Updating the Apex One Server	Certified Safe Software list	

Further Information:

For More information, or to book your course, please call us on 00 966 92000 9278

training@globalknowledge.com.sa

www.globalknowledge.com/en-sa/

Global Knowledge - KSA, 393 Al-Uroubah Road, Al Worood, Riyadh 3140, Saudi Arabia