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:OperationsDeploymentSecurity ResponseCompliance

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:

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:

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

Apex One Overview

- Trend Micro solutions
- Key features of Apex One
- Apex One components
- Deployment methods
- Threat detection

Apex One Server

- Apex One Server tasksA
- pex One Server services and components
- Configuration repositories
- Installing/upgrading Apex One Server
- Apex One plug-ins and utilities

Apex One Web Management Console

- Logging into the console
- Integrating with Active Directory
- Creating new administrative accounts

Security Agents

- Security Agent tasks
- Security Agent services and components
- Security Agent tree
- Installing Agents
- Migrating from other endpoint security software
- Agent-to-Server/Server-to-Agent communication
- Endpoint location
- Moving Security Agents
- Uninstalling Security Agents
- Agent settings and grouping
- Agent self-protection
- Agent privileges

Managing Off-Premise Agents

- Protection features
- Installing the Apex One Edge Relay Server
- Registering the Apex One Edge Relay Server
- Edge Relay Server and external Agent communication
- Edge Relay Server digital certificates

Keeping Apex One Updated

- ActiveUpdate
- Updating the Apex One Server
- Updating Security Agents
- Update Agents
- Security compliance

Trend Micro Smart Protection

- Smart Protection services and sources
- Configuring the Smart Protection source

Protecting Endpoint Computers from Malware

- Scanning for malware
- Scan settings
- Quarantining malware
- Smart Scan
- Spyware/grayware protection
- Preventing outbreaks

Protecting Endpoint Computers Through Behavior Monitoring

- Malware behavior blocking
- Ransomware protection
- Anti-exploit protection
- Fileless malware protection
- Newly encountered program detection
- Event monitoring
- Behavior monitoring exceptions

Protecting Endpoint Computers from Unknown Threats

- Common Vulnerabilities and Exposures exploits
- Predictive machine learning
- Offline predictive machine learning

Detecting Emerging Malware Through Trend Micro™ Connected Threat Defense

- Connected Threat Defense requirements
- Deep Discovery Analyzer
- Suspicious Objects

Blocking Web Threats

- Web reputation
- Detecting suspicious connections
- Protecting against browser exploits

Protecting Endpoint Computers Through Traffic Filtering

- Firewall filtering
- Application filtering
- Certified Safe Software list
- Stateful inspection
- Intrusion Detection System
- Firewall policies and profiles

Preventing Data Leaks on Endpoint Computers

- Data Loss protection
- Installing Data Loss protection
- Configuring data identifiers, data loss prevention templates and policies
- Device control

Deploying Policies Through Apex Central

- Apex Central
- Apex Central management modes
- Managing Apex One policies in Apex Central
- Data Discovery policies

Blocking Unapproved Applications on Endpoint Computers

- Integrated Application Control
- Application Control criteria
- Implementing Application Control
- User-based Application Control
- Lockdown Mode
- Best practices

Protecting Endpoint Computers from Vulnerabilities

- Integrated Vulnerability Protection
- Vulnerability Protection Pattern
- Implementing Vulnerability Protection
- Network Engine settings

Detecting and Investigating Security Incidents on Endpoint Computers

- Integrated Endpoint Sensor
- Endpoint Detection and Response
- Apex One Incident Response Model
- Managed Detection and Response

Troubleshooting Apex One

- Debugging the Apex One Server and Agents
- Troubleshooting communication issues
- Troubleshooting virus infection
- Troubleshooting Apex One services
- Troubleshooting sample submission

Further Information:

For More information, or to book your course, please call us on Head Office Tel.: +974 40316639

training@globalknowledge.qa

www.globalknowledge.com/en-qa/

Global Knowledge, Qatar Financial Center, Burj Doha,Level 21, P.O.Box 27110, West Bay, Doha, Qatar