Trend Micro™ OfficeScan Training for Certified Professionals

Course Description:

In this course, you will learn how to use Trend Micro™ OfficeScan. This course provides information about the basic architecture and functionality of OfficeScan, as well as deployment scenarios, and troubleshooting options. Through hands-on labs, you will install and configure different OfficeScan security features and administration options, to learn the various functions that an administrator needs to know for a successful implementation and long-term maintenance.

Target Audience:

This course is designed for IT professionals who are responsible for protecting networks from any kind of networked, endpoint, or cloud security threats.

The individuals who will typically benefit the most include:

- System administrators
- Network engineers
- Support Engineers
- Integration Engineers
- Solution & Security Architects

Course Prerequisites:

Before you take this course, Trend Micro recommends that you have a working knowledge of their products and services, as well as basic networking concepts and principles.

You should also have a working knowledge of the following products:

- Windows servers and clients
- Microsoft Internet Information Server (IIS)
- General understanding of malware

Course Topics:

- OfficeScan Overview
  - New Features and Enhancements in OfficeScan XG
    - Architecture Overview (OfficeScan Server and Agents)
  - Key Features and Benefits
  - Footprint
    - Services and Major Components
    - Configuration Repository and Database

- Installation
  - OfficeScan Server and Agent Installations
  - Upgrade Options
  - Server Migration
  - Agent Installation Methods, Uninstalls and Post Installation Tasks

- Communication and Administration
  - Ports and Protocols
  - Authentication
  - Management Console
  - Users, Roles and Grouping
- Protection
  - Smart Protection Network and Smart Protection Servers
  - Virus Protection
  - File Reputation
  - Spyware/Grayware Protection
  - Firewall Protection
  - Web Threat Protection
- Communication and Admin
  - Agent/Server Communications
  - Troubleshooting
  - Authentication
  - Ports and Protocols
  - Console Access and Roles
  - Unmanaged Endpoints
  - Agent Grouping and Settings
  - Offline Agents
  - OfficeScan Edge Relay for Off Premise Protection

- Update
  - Server and Agent Updates
  - Update Methods and Sources
  - Downloading and Deploying
  - Rollbacks

- Protection
  - Smart Protection Network and Servers
  - Virus Protection
  - File Reputation
  - Advanced Threat Scan Engine (ATSE) Scan
  - Spyware/Grayware Protection
  - Damage Clean-up
  - Firewall
  - Web Threat Protection

- Additional Protection
  - Behaviour Monitoring (including Unauthorized Change Prevention)
  - Census (Behaviour Monitoring)
  - Ransomware Protection
  - Memory Scanning and Browser Exploit Solution
  - Suspicious Connection Services
  - Predictive Machine Learning

- Data Protection (Data Loss Prevention)
  - Architecture and Installation
  - DLP Agent
  - Device and Digital Asset Control
  - DLP Logging and Debugging
  - Trend Micro Control Manager DLP Management for OfficeScan

- Connected Threat Defense
  - Threat Response Flow
  - Registering Trend Micro Control Manager to OfficeScan
  - Configuring Suspicious Objects
  - Agent Sample Submission to Deep Discovery Analyzer (DDAn)
  - Suspicious Object Logs

- Troubleshooting
  - Debugging OfficeScan Server and Agents
  - Determining Virus Detections (Infection Channel)
  - Enabling SSAPI Logs
  - Debugging Common Issues
    - Firewall
    - Integrated Web Reputation Service
    - Unauthorized Change Prevention Service
    - Web Reputation Service
    - OfficeScan Edge Server
    - Certificates
    - Sample Submission and Suspicious Objects
  - Smart Protection Server Best Practises