Trend Micro™ Deep Discovery Training for Certified Professionals

Course Description

Trend Micro™ Deep Discovery Training for Certified Professionals is a three-day, instructor-led training course where participants will learn how to deploy and manage a Trend Micro™ Deep Discovery threat protection solution using:

- Trend Micro™ Deep Discovery Inspector
- Trend Micro™ Deep Discovery Analyzer
- Trend Micro™ Deep Discovery Email Inspector

Participants explore key concepts and methodologies of using a blend of Deep Discovery solutions for a more complete approach to network security. This course details the architecture, deployment options, threat management and system administration fundamentals, as well as troubleshooting and best practices, for all three products.

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 choose to complete the certification examination to obtain designation as a **Trend Micro Certified Professional for Deep Discovery**.

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
- Firewalls, Web Application Firewalls, Packet Inspection devices
- General understanding of malware

Participants are required to bring a laptop computer with a screen resolution of at least 1980 x 1080 or above; a display size of 15" or above is recommended.

Course Topics

Course topics are divided into the following lessons.

Introduction

- Evolving Threats
- Traditional Security
- Anatomy of a Targeted Attack
- Point of Entry - Spear Phishing
- How Long Can Targeted Attacks Stay Hidden?
- Why Monitor Your Network?
- Why Deep Discovery?

Deep Discovery Solution Overview

- What is Deep Discovery?
- Deep Discovery Attack Detection
- Deep Discovery Threat Detection Technologies
- Deep Discovery Solution Map
  - Trend Micro Deep Discovery Inspector
  - Trend Micro Deep Discovery Analyzer
  - Trend Micro Deep Discovery Email Inspector
  - Control Manager
  - Custom Threat Defense
  - Deep Discovery Director

Deep Discovery Inspector

- Key Features and Benefits
- Network Setup
- Form Factors
- Deep Discovery Inspector Models

Deep Discovery Inspector Installation and Configuration

- Installation Design
- Deployment Example and Scenarios
- System Requirements
- Installing Deep Discovery Inspector
  - Information Provisioning for Setup
  - Defining Architecture and Traffic to Capture
  - Obtaining ISOs, Hot Fixes/Patches
  - Performing an Installation
  - Configuring Initial System Settings (Pre-Configuration Console)
  - Finalizing Deep Discovery Inspector Configuration (Web Console)
  - Testing the Deployment
  - Viewing Installation Logs
  - Connecting Deep Discovery Inspector to Deep Discovery Director

Threat Detect Technologies

- Network Content Inspection Engine (NCIE / VSAPI)
- Advanced Threat Scan Engine (ATSE / VSAPI)
- Network Content Inspection Engine (NCIE / VSAPI)
- Network Content Correlation Engine (NCCE / CAV)
- Virtual Analyzer
- Census
- Certified Safe Software Service (CSSS / GRID)
- Trend Micro URL Filtering Engine (TMUFE)
- Network Reputation with Smart Protection Network
- Mobile Application Reputation Service (MARS)

Deep Discovery Inspector Management and Administration

- Administration Methods
- Default Accounts
- Threat Management and Configuration
- System Management and Configuration
- Monitoring System Performance and Resources
- Troubleshooting Resource Issues

Deep Discovery Inspector Logs and Reports

- Accessing System Logs
- Debug Logs
- Determining Log Entities
- Reporting Logs - Event Classification
- Debug Portal
- Threat Reports

Virtual Analyzer

- Virtual Analyzer Functionality
- What is Virtual Analyzer Looking For?
- Virtual Analyzer Components
- Process Flow for Samples
- Overall Sample Ratings and Risk Level
- Virtual Analyzer Outputs
- Virtual Analyzer Report
- How to Explain a Malicious Result
- Sending Files to Virtual Analyzer for Analysis
- Virtual Analyzer Feedback in Deep Discovery Inspector
- Importing a Custom Sandbox into Deep Discovery Inspector for use by the Virtual Analyzer

Deep Discovery Analyzer Installation and Configuration

- Information Provisioning
- Defining the Architecture
- Obtaining ISOs, Hot Fixes/Patches
- Performing the Installation
- Configuring Initial System Settings
- Configuring Final Settings for Deep Discovery Analyzer
- Testing the Deployment

Deep Discovery Analyzer Administration

- Console Overview
- General Administrative Tasks
- Troubleshooting

Deep Discovery Email Inspector

- Functionality
- Supported Hardware
- Deployment Modes
- Ports Used
- Summary of Operation Modes
- Threat Detection in Deep Discovery Email Inspector

Deep Discovery Email Inspector Installation and Configuration

- Information Provisioning
- Defining the Architecture
- Obtain ISOs, Hot Fixes/Patches
- Performing the Installation
- Completing Pre-Configuration
- Configuring Final Deep Discovery Email Inspector Settings
- Testing the Deployment

Deep Discovery Email Inspector Administration

- Management Console Overview
- How to View Detections
- Configuring Policies
- Setting up Recipient Notifications
- Defining Email Message Tags
- Configuring Redirects (Non-Scannable Attachments)
- Adding Policy Exceptions
- Configuring Alerts
- Generating Reports
- Accessing Log Files
- System Administration and Management
- Performing System Maintenance Tasks

Threat Connect

- Content
- Using Threat Connect
- Report Content

Connected Threat Defense

- Integration is Key to Effective Security
- Connected Threat Defense Requirements
- Connected Threat Defense Components
- Suspicious Objects
- Handling Suspicious Objects
- Trend Micro Control Manager
- Integrating Deep Discovery Inspector with Control Manager

Integration

- Open Architecture
- Deep Discovery Inspector Integration
- Integration with Syslog Servers and SIEM Systems
- Third-Party Blocking Integration
- Deep Discovery Analyzer Integration