Trend Micro™ Deep Discovery Training Advanced Threat Detection 2.0 for Certified Professionals

Course Description

Trend Micro™ Deep Discovery Training Advanced Threat Detection 2.0 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 security 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 and 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.

Product Overview

- Introduction to Trend Micro Solutions
- Deep Discovery Key Features
- Deep Discovery Solution Platforms
  - Trend Micro Deep Discovery Inspector
  - Trend Micro Deep Discovery Analyzer
  - Trend Micro Deep Discovery Email Inspector
  - Deep Discovery Director
  - Trend Micro Control Manager
- Key Business Needs for Network Defense

Deep Discovery Solution Overview

- Evolving Threat Landscape
- Phases of a Targeted
- Deep Discovery Threat Detection Overview

Deep Discovery Inspector Product Overview

- Introduction
- Key Features
- Network Setup
- Form Factors
- Deep Discovery Inspector Requirements
- Installation Design
- Positioning Deep Discover Inspector in the Network

Installing and Configuring Deep Discovery Inspector

- Information Provisioning for Setup
- 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
- Operational Settings and Boot Options

Threat Detect Technologies

- Network Content Inspection Engine (NCIE / VSAPI)
- Advanced Threat Scan Engine (ATSE / VSAPI)
- Network Content Correlation Engine (NCCE / CAV)
- Virtual Analyzer
- Community File Reputation (Census)
- Trend Micro Cloud Sandbox Service
- Community Domain/IP Reputation Service (Domain Census)
- Certified Safe Software Service (CSSS / GRID)
- Trend Micro URL Filtering Engine (TMUFE)
- Network Reputation with Smart Protection Network
- Mobile Application Reputation Service (MARS)
- TrendX Machine Learning
- Threat Detection Overview
- Processing Stages

Virtual Analyzer

- Introduction
- Key Features and Functionality
- What is Virtual Analyzer Looking For?
- Virtual Analyzer Components
- Sending Files to Virtual Analyzer for Analysis
- Virtual Analyzer Process Flow
- Virtual Analyzer Stages
- Overall Sample Ratings and Risk Level
- Viewing Detection Details
- Interpreting Analysis Results
- Virtual Analyzer Feedback Blacklist
- Hosts with C&C Callbacks
- Deny/Allow List
- Virtual Analyzer Settings
- Importing a Custom Sandbox into Deep Discovery Inspector for use by the Virtual Analyzer

Deep Discovery Inspector Administration

- Logging In
- Dashboard
- Analyzing Detected Threats
- Viewing Key Fields in Events
- Detection Type Examples
- Running Reports and Obtaining Threat Detection Metrics
- System Administration Functions

Deep Discovery Analyzer Product Overview

- Introduction
- Key Features
- Network Setup
- Form Factors
- Required Services and Port Information
- Uniquely Identifying Samples
- Product Integration

Installing and Configuring Deep Discovery Analyzer

- 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

- Logging In
- User Accounts
- Web Console Overview
- Analyzing Samples and Results
- Submitting Samples to Deep Discovery Analyzer
- Virtual Analyzer Report
- Managing Suspicious Objects List
- Exceptions
- Deep Discovery Analyzer Sandbox Management
- Reports
- Alerts
- Managing the System
  - Updating Components, Creating User Accounts, Performing Backups, Troubleshooting etc.

Deep Discovery Email Inspector

- Introduction
- Key Features
- License Management
- Form Factors
- Deployment Modes
- Ports Used
- Scanning Technologies
- Deep Discovery Email Inspector Scanning
- Risk Levels

Installing and Configuring Deep Discovery Email Inspector

- Information Provisioning
- Defining the Architecture
- Obtaining ISOs, Hot Fixes/Patches
- Performing the Installation
- Configuring Initial Settings
- Completing the Configuration for Deep Discovery Email Inspector
- Additional Tasks for Installing
- Testing Your Deployment

Deep Discovery Email Inspector Administration

- Logging In
- Accounts
- Web Console Overview
- Dashboard and Widgets
- Managing Threat Detections
- Steps for Analyzing Detections
- Configuring Policies
- Setting up Recipient Notifications
- Defining Email Message Tags
- Configuring Time-of-Click Protection
- Configuring Business Email Compromise Protection
- Configuring Redirects (for Unscannable Attachments)
- Generating Reports
- Accessing Log Files
- End User Quarantine (EUQ)
- Performing Administrative Tasks
  - Performing Component and Product Updates, Backing Up, Troubleshooting etc.

Deep Discovery Director Product Overview

- Introduction
- Form Factors and Requirements
- Planning a Deployment
- Installing Deep Discovery Director
- Deep Discovery Appliance Management
- Viewing Detections

Connected Threat Defense Overview

- Connected Threat Defense Components
- How Connected Threat Defense Works
- Integration with Control Manager
- Suspicious Objects and Community Exchanged IOCs

Appendices

- What's New in Deep Discovery Inspector 5.0?
- What's New in Deep Discovery Analyzer 6.0?
- What's New in Deep Discovery Email Inspector 3.0?
- Monitoring VM Traffic with Deep Discovery Inspector
- Trend Micro Threat Connect
- Integration
- Deep Discovery Inspector Supported Protocols