Trend Micro

DEEP DISCOVERY™ ADVANCED THREAT DETECTION 2.1 TRAINING FOR CERTIFIED PROFESSIONALS

In this course participants will learn how to plan, deploy, and manage a Trend Micro Deep Discovery threat detection solution using:

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

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

CERTIFICATIONS AND RELATED EXAMINATIONS:

Upon completion of this course, participants may choose to complete the certification exam to obtain designation as a Trend Micro Certified Professional for Deep Discovery Advanced Threat Detection.

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.

COURSE OBJECTIVES:

Upon completion of this course, you will be able to:

- Describe the purpose, features, and capabilities of Trend Micro Deep Discovery Advanced Threat Detection solutions
- Install, configure and use security management and administration settings for Deep Discovery Advanced Threat Detection solutions
- Attempt the Trend Micro Certified Professional for Deep Discovery Certification Exam

WHY CHOOSE VERACOMP EDUCATION

- Hands-on instruction and best practice advice from our experienced trainers
- With Trend Micro product certifications, you have the skills to deploy and manage their leading security solutions
- By sharpening your skills, you are more able to detect and respond to the latest attacks

Target Audience:

This course is designed for IT professionals who are responsible for protecting networks from any kind of network, 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

Available courses from Trend Micro's official curriculum:

- Trend Micro Certified Professional for Apex One
- Trend Micro Certified Professional for Deep Security
- Trend Micro Certified Professional for Deep Discovery

Training

Price: 950 EUR

* 3 days course, materials and certification included, lunch and refreshments provided

Need customized course?

No problem! We can deliver course according to your preferred topic, course location or length.

TREND MICRO™ Securing Your Journey to the Cloud

veracomp we inspire IT

DETAILED COURSE OUTLINE:

The course topics in this training 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
- The evolving threat landscape
- Phases of a targeted attack
- Deep Discovery threat detection overview

Deep Discovery Inspector Product Overview
- 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, hotfixes/patches
- Performing an installation
- Configuring initial system settings (preconfiguration 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)/virus-scanning application program interface (VSAPI)
- Advanced Threat Scan Engine (ATSE)/virus-scanning application program interface (VSAPI)
- Network content correlation engine (NCEE)/computer-aided verification (CAV)
- Virtual analyzer
- Community file reputation (census)
- Trend Micro cloud sandbox service
- Community domain/internet protocol (IP) reputation service (domain census)
- Certified safe software service (CSSS)/global resource information database (GRID)
- URL filtering engine
- Network reputation with Trend Micro™ Smart Protection Network™
- Mobile application reputation service (MARS)
- Trend machine learning
- Threat detection overview
- Processing stages

Virtual Analyzer
- 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 command and control (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
- Key features
- Network setup
- Form factors
- Required services and port information
- Uniquely identifying samples
- Product integration

Information Provisioning
- Defining the architecture
- Obtaining ISOs, hotfixes/patches
- Performing the installation
- Configuring initial system settings
- Configuring final settings for Deep Discovery Analyzer
- Testing the deployment

TREND MICRO™ Securing Your Journey to the Cloud

veracomp we inspire IT

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, and accessing the Debug Portal, and etc.

Deep Discovery Email Inspector

- Key features
- Form factors
- Deployment modes
- Multi-target-application (MTA), blind carbon copy (BCC), switch port analyzer (SPAN)/ test access point (TAP)
- 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, hotfixes/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 (BEC) protection
- Configuring redirects (for un-scannable attachments)
- Generating reports
- Accessing log files
- End user quarantine (EUQ)
- Performing administrative tasks
- Component and product updates, backup/restore, debug, and etc.

Deep Discovery Director Product Overview

- 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 indicators of compromise (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 virtual machine traffic with Deep Discovery Inspector
- Trend Micro Threat Connect
- Integration
- Deep Discovery