Trend Micro™

DEEP DISCOVERY™ ADVANCED THREAT DETECTION 3.0 TRAINING FOR CERTIFIED PROFESSIONALS

COURSE DESCRIPTION:

Trend Micro™ Deep Discovery™ Advanced Threat Detection 3.0 Training for Certified Professionals is a three-day, instructor-led training course where participants will learn how to plan, deploy, and manage a Deep Discovery threat detection solution using:

- Trend Micro™ Deep Discovery™ Inspector
- Trend Micro™ Deep Discovery™ Analyzer
- Trend Micro™ Deep Discovery™ Director
- Trend Micro™ Deep Discovery™ Director - Network Analytics

Participants explore key concepts and methodologies of using a blend of Deep Discovery solutions for a more complete approach to network security. This course provides a variety of hands-on lab exercises, allowing each student to put the lesson content into action. There will be an opportunity to setup and configure various Deep Discovery solution management and administration features and test their functionality using the virtual labs.

A comprehensive look is provided on the purpose, features, and capabilities of Deep Discovery network security solutions, including recommendations on best practices and general troubleshooting steps for a successful implementation and long-term maintenance of a Deep Discovery environment.

The course also explores various deployment considerations and requirements needed to tie Deep Discovery solutions into other Trend Micro products to provide synchronized threat intelligence sharing for advanced threat detection.

KEY INFORMATION	
Course Title:	Trend Micro Deep Discovery Advanced Threat Detection 3.0 Training for Certified Professionals
Product ID:	TRNN1040 or TRNM0003
Course Length:	Three Days
Level:	Professional
Delivery Language:	English
To Enroll:	Existing account holders can visit the Trend Micro Education Portal for a list of available classes. For more information about how to create an account, please visit **trendmicro.com/education**

CERTIFICATIONS AND RELATED EXAMINATIONS:

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 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.

Experience with the following products and technologies is also necessary:

- 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 recommended screen resolution of at least 1980 x 1080 or above, and a display size of 15" or above.

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

COURSE OBJECTIVES:

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

- Describe the purpose, features, and capabilities of Deep Discovery advanced threat detection solutions
- Configure Deep Discovery Inspector, and enable threat detection
- Setup and use administrative and security management features in:
  - Deep Discovery Inspector
  - Deep Discovery Analyzer
  - Deep Discovery Director
- Explain how Connected Threat Defense™ works
- Describe key features of Deep Discovery Director and how to integrate with other Deep Discovery products for centralized management and visibility

WHY CHOOSE TREND MICRO EDUCATION

- Hands-on instruction from Trend Micro certified trainers
- With Trend Micro product certifications, you have the skills to deploy and manage our leading security solutions
- On demand or in a classroom, we have the right courses for you
- By sharpening your skills, you are in a position to better detect and respond to the latest attacks

For More Information:

Please contact Trend Micro Education for additional information

education@trendmicro.com

DETAILED COURSE OUTLINE:

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

Product Overview

- Trend Micro solutions
- Trend Micro Network Defense
  - Key requirements for Trend Micro Network Defense
  - Threat classifications
  - Trend Micro Network Defense solutions
- Deep Discovery
  - Product family
  - Deep Discovery capabilities
  - Deep Discovery threat detection technology overview

Deep Discovery Inspector

- Network requirements
- Deep Discovery Inspector network connections
- Services accessed by Deep Discovery Inspector
- Deep Discovery Inspector deployment topologies
  - Single connection–single Deep Discovery Inspector
  - Multiple connections–single Deep Discovery Inspector
  - Multiple connections–multiple Deep Discovery Inspectors
  - Inter-VM traffic
  - Gateway proxy servers
  - Caveats for deploying Deep Discovery Inspector only at ingress/egress points
- Understanding the attack cycle

Configuring Deep Discovery Inspector

- Pre-configuration console
- Configuring network settings
- Configuring system settings
- Performing administration tasks
- Deep Discovery Inspector Virtual Analyzer
- Configuring Deep Discovery Inspector detection rules
- Avoiding false positives
- Troubleshooting Deep Discovery Inspector
  - Check network link status from web console
  - Verifying back-end services
  - Testing with demo rules
  - Packet capturing
  - Verifying if network traffic is received
  - Testing ATSE-based detections
  - Testing malicious URLs
  - Verifying detected threats
  - Checking system performance

Analyzing Detected Threats in Deep Discovery Inspector

- Using the dashboard to view detected threats
- Using the detections' menu to view and analyze detected threats
  - Identifying affected hosts in attacks
  - Viewing affected hosts information
  - Viewing detection details
  - Viewing all Deep Discovery Inspector detections
- Obtaining key information for analyzing threat detections
  - Detection severity information
  - Attack phase information
  - Detection type information
- Working with suspicious objects deny list
  - Block action for deny list
  - Allow list
  - Suspicious objects risk rating
- Viewing hosts with command and control callbacks
- Virtual Analyzer settings
  - Controlling file submissions to Virtual Analyzer
  - Virtual Analyzer cache
  - Virtual Analyzer sample processing time
  - File submission issues (not being sent to Virtual Analyzer)

Deep Discovery Analyzer

- Key features
- Deep Discovery Analyzer specifications
- Ports used
- What is Deep Discovery Analyzer looking for?
- Deep Discovery Analyzer sandbox
- Scanning flow
  - Sandbox analysis flow
  - Post-sandbox analysis flow
  - Virtual Analyzer outputs
- Configuring network settings for Deep Discovery Analyzer
- Using the Deep Discovery Analyzer web console
- Performing system management functions
- Performing Deep Discovery Analyzer sandbox tasks
- Product compatibility and integration
- Submitting samples to Deep Discovery Analyzer
- Viewing sample submission details
- Obtaining full details for analyzed samples
- Managing the suspicious objects list
- Interpreting results
- Generating reports
- Using alerts
- Preparing and importing a custom sandbox

Deep Discovery Director

- Deep Discovery Director requirements
- Product interoperability
- Planning a deployment
- Installing Deep Discovery Director
- Configuring network settings in the pre-configuration console
- Managing Deep Discovery Director
- Configuring deployment plans
- Managing threat detections
- Sharing advanced threats and indicators of compromise (IOCs) through STIX and TAXII

Deep Discovery Director - Network Analytics

- Threat sharing
- Deploying Deep Discovery Director - Network Analytics
  - Pre-deployment checklist
  - System requirements
  - Installing Deep Discovery Director - Network Analytics on a VMware® virtual machine
- Managing Deep Discovery Director - Network Analytics
  - Accessing Deep Discovery Director - Network Analytics settings
  - Registering to Deep Discovery Inspector
  - Adding a syslog server
  - Configuring additional settings
- Correlation overview
  - Metadata samples
- Using correlation data for threat analysis
  - Viewing correlation data (correlated events)
- Analyzing correlation data information
  - Reviewing correlation data summary
  - Viewing the correlation data graph
- Viewing correlation data for suspicious objects

Preventing Targeted Attacks Through Connected Threat Defense

- Connected Threat Defense life cycle
- Combating targeted attacks with Connected Threat Defense
- Key benefits of Connected Threat Defense
- Requirements for Connected Threat Defense
- Connected Threat Defense architecture
- Suspicious object list management
- Setting up Connected Threat Defense
- Suspicious objects handling process
- Tracking suspicious objects

Appendices

- What's new
  - Deep Discovery Inspector 5.5
  - Deep Discovery Analyzer 6.5
  - Deep Discovery Director 5.0
  - Deep Discovery Director - Network Analytics as a Service 5.0
- Trend Micro Threat Connect
- Trend Micro product integration
- Deep Discovery Inspector supported protocols
- Installing and configuring Deep Discovery Inspector
- Deep Discovery Threat Detection technologies
- Creating sandboxes

Securing Your Connected World