TREND MICRO | Authorized Training Center

Trend Micro™ Deep Discovery™ Advanced Threat Detection 4.0 Training for Certified Professionals

COURSE DESCRIPTION:

Trend Micro™ Deep Discovery™ Advanced Threat Detection 4.0 Training for Certified Professionals is a three-day, instructor-led training course where participants will learn how to use Deep Discovery Advanced Threat Protection solutions to detect, analyze, and respond to advanced threats and targeted attacks.

Participants explore key concepts and methodologies using the following blend of Deep Discovery products for a more complete approach to network security:

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

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 set up and configure various Deep Discovery management and administration features and explore their functionality using a virtual lab environment.

A comprehensive look at the purpose, features, and capabilities of Deep Discovery Advanced Threat Protection solutions. This includes recommendations on best practices and general troubleshooting steps for a successful implementation, along with long-term maintenance of Deep Discovery solutions in your environment.

The course also explores various deployment considerations and requirements needed to tie Deep Discovery into various other Trend Micro solutions, like Trend Micro Vision One™, to enhance threat hunting and intelligence sharing, for better threat detection functionality.

KEY INFORMATION:

Course Title	Trend Micro Deep Discovery Advanced Threat Detection 4.0 Training for Certified Professionals
Product ID	TRNN1040 or TRNM0003
Course Length	Three Days
Level	Professional
Delivery Language	English

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.

COURSE OBJECTIVES:

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

- Describe the purpose, features, and capabilities of Trend Micro's Deep Discovery advanced threat detection solutions
- Deploy and configure the following Deep Discovery products:
  - Deep Discovery Analyzer
  - Deep Discovery Inspector
  - Deep Discovery Email Inspector
  - Deep Discovery Director
- Analyze detected threats and share threat intelligence with Incident Response/Security Ops Centres
- Create custom sandboxes for virtual analysis of suspicious objects
- Manage suspicious objects and share threat intelligence with integrated security products
- Centrally manage firmware and component updates through Deep Discovery Director

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

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
- Security Operation Centres
- Solution and Security Architects

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

Product Overview

- Product Portfolios
- Network Detection
- Trend Micro™ Deep Discovery™ Product Family

Deep Discovery Analyzer

- Network Setup
- What is Deep Discovery Analyzer Looking For?
- Creating and Importing a Sandbox Images
- Deep Discovery Analyzer Tools
- Submitting Samples to Deep Discovery Analyzer
- Suspicious Objects List Management
- MITRE ATT&CK™ Framework Tactics and Techniques

Deep Discovery Inspector

- Network Service Diagnostics
- Deep Discovery Inspector Deployment Topologies
- Phases of a Targeted Attack
- Case Study: APT36 (Earth Karkaddan) Attack Chain and Malware Arsenal
- Indicators of Compromise
- Deep Discovery Threat Detection Technologies

Deep Discovery Inspector Best Practice and Configuration

- Deploying Deep Discovery Inspector
- Configuring Initial Network Settings
- Best Practice Configurations and Management
- Working with Logs and Reports
- Troubleshooting (Packet Capturing)

Analyzing Detected Threats in Deep Discovery Inspector

- Working with Threat Dashboards
- Obtaining Key Information for Analyzing Threat Detections
- Viewing Hosts with Command-and-Control Callbacks
- Connecting to a Virtual Analyzer for Sandbox Analysis
- Dealing with Aggressive or False Positive Detections

Deep Discovery Email Inspector

- Deployment Technologies
- Email Scanning Technologies
- Integration with Trend Miro Products

Deploying Deep Discovery Email Inspector

- Installing and Configuring Deep Discovery Email Inspector
- Network Configuration
- Virtual Analyzer Sandbox Configuration
- Troubleshooting

Deep Discovery Email Inspector Administration

- Analyzing Detections
- Policy Management
- Configuring Scanning / Analysis
- Policy Management
- Configuring Virtual Analyzer for Sandbox Analysis
- Using Debug Functions

Deep Discovery Director

- Installing Deep Discovery Director
- Connecting Deep Discovery Products to Deep Discovery Director
- Sending Logs to a Syslog Server
- Deployment Plans
- Managing Threat Detections through Deep Discovery Director
- Viewing Email Messages with Malicious or Suspicious Content
- Configuring Rules for Detection
- Threat Intelligence Interoperability (STIX,TAXII)

Trend Micro Vision One™ Overview

- Trend Micro XDR
- Trend Micro Vision One
- Trend Micro Vision One Apps
- Trend Micro™ Managed XDR Service

Deep Discovery Inspector and Trend Micro Vision One

- Deploying Network Inventory Service
- Downloading the Deep Discovery Inspector Image
- Creating a Virtual Machine for Deep Discovery Inspector on VMware ESXi
- Configuring Deep Discovery Inspector Network Settings
- Connecting Deep Discovery Inspector withTrend Micro Vision One
- Deploying Trend Micro Service Gateway
- Connecting Deep Discovery Inspector with Service Gateway

Appendices

- Deep Discovery Threat Detection Technologies
- Trend Micro Product Integration
- Creating Sandboxes