



Trend Micro Deep Discovery Training for Certified Professionals

Duration: 3 Days **Course Code: TMDD**

Overview:

™ 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.

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

Objectives:

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

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.

Content:

Product Overview :	Detection severity information	Analytics
Trend Micro solutions	Attack phase information	Threat sharing
Trend Micro Network Defense	Detection type information	Deploying Deep Discovery Director –
Key requirements for Trend Micro Network Defense	Working with suspicious objects deny list	Network Analytics
Threat classifications	Block action for deny list	Pre-deployment checklist
Trend Micro Network Defense solutions	Allow list	System requirements
Deep Discovery	Suspicious objects risk rating	Installing Deep Discovery Director -
Product family	Viewing hosts with command and control callbacks	Network Analytics on a VMware virtual machine
Deep Discovery capabilities	Virtual Analyzer settings	Managing Deep Discovery Director –
Deep Discovery threat detection technology overview	Controlling file submissions to Virtual Analyzer	Network Analytics
Deep Discovery Inspector :	Virtual Analyzer cache	Accessing Deep Discovery Director –
Network requirements	Virtual Analyzer sample processing time	Network Analytics settings
Deep Discovery Inspector network connections	File submission issues (not being sent to Virtual Analyzer)	Registering to Deep Discovery Inspector
Services accessed by Deep Discovery Inspector	Deep Discovery Analyzer :	Adding a syslog server
Inspector	Key features	Configuring additional settings
Deep Discovery Inspector deployment topologies	Deep Discovery Analyzer specifications	Correlation overview
Single connection—single Deep Discovery Inspector	Ports used	Metadata samples
Inspector	What is Deep Discovery Analyzer looking for?	Using correlation data for threat analysis
Multiple connections—single Deep Discovery Inspector	Deep Discovery Analyzer sandbox	Viewing correlation data (correlated events)
Discovery Inspector	Scanning flow	Analyzing correlation data information
		Reviewing correlation data summary

Multiple connections—multiple Deep	Sandbox analysis flow	Viewing the correlation data graph
Discovery Inspectors	Post-sandbox analysis flow	Viewing correlation data for suspicious objects
Inter-VM traffic	Virtual Analyzer outputs	Preventing Targeted Attacks Through :
Gateway proxy servers	Configuring network settings for Deep	Connected Threat Defense
Configuring Deep Discovery Inspector :	Discovery Analyzer	Connected Threat Defense life cycle
Pre-configuration console	Using the Deep Discovery Analyzer	Combating targeted attacks with
Configuring network settings	web console	Connected Threat Defense
Configuring system settings	Performing system management functions	Key benefits of Connected Threat Defense
Performing administration tasks	Performing Deep Discovery Analyzer	Requirements for Connected
Deep Discovery Inspector Virtual Analyzer	sandbox tasks	Threat Defense
Configuring Deep Discovery Inspector detection rules	Product compatibility and integration	Connected Threat Defense architecture
Avoiding false positives	Submitting samples to Deep Discovery	Suspicious object list management
Troubleshooting Deep Discovery Inspector	Analyzer	Setting up Connected Threat Defense
Check network link status from web console	Viewing sample submission details	Suspicious objects handling process
Verifying back-end services	Obtaining full details for analyzed samples	Tracking suspicious objects
Testing with demo rules	Managing the suspicious objects list	Appendices :
Packet capturing	Interpreting results	What's new
Verifying if network traffic is received	Generating reports	Deep Discovery Inspector 5.5
Testing ATSE-based detections	Using alerts	Deep Discovery Analyzer 6.5
Testing malicious URLs	Preparing and importing a	Deep Discovery Director 5.0
Verifying detected threats	custom sandbox	Deep Discovery Director - Network

Checking system performance Caveats for deploying Deep Discovery Inspector	Deep Discovery Director:	Analytics as a Service 5.0
Inspector only at ingress/egress points	Deep Discovery Director requirements	Trend Micro Threat Connect
Understanding the attack cycle	Product interoperability	Trend Micro product integration
Analyzing Detected Threats in Deep Discovery Inspector :	Planning a deployment	Deep Discovery Inspector supported protocols
Using the dashboard to view detected threats	Installing Deep Discovery Director	Installing and configuring
Using the detections' menu to view and analyze detected threats	Configuring network settings in the preconfiguration console	Deep Discovery Inspector
Identifying affected hosts in attacks	Managing Deep Discovery Director	Deep Discovery Threat
Viewing affected hosts information	Configuring deployment plans	Detection technologies
Viewing detection details	Managing threat detections	Creating sandboxes
Viewing all Deep Discovery Inspector detections	Sharing advanced threats and indicators of compromise (IOCs) through STIX and TAXII	
Obtaining key information for analyzing threat detections	Deep Discovery Director - Network :	

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo