Trend Micro Deep Discovery Advanced Threat Detection 3.0 Edition 3 for Certified Professionals

Category: Networking & Security | **Vendor:** Trend Micro

Duration: 24.00 hours (3 days) **19.5 CPD Hours** **Rating:** ⭐ 4.6 (5,878 reviews)

Course Information

Delivery Format:	Instructor Led - Online
Certification:	Certified Professionals Participants explore key concepts and methodologies of using a blend of Deep

Course Overview

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.

About This Course

Product Overview

- Trend Micro solutions
- Trend Micro Network Defense

- Key requirements for Trend Micro Network Defense
- Threat classifications
- Trend Micro Network Defense solutions
- Trend Micro Deep Discovery

- Product family
- Deep Discovery capabilities
- Deep Discovery Integration

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 point
- Understanding the attack cycle
- Phases of a targeted attack
- Case study: Pawn storm spear-Phishing
- Deep discovery Threat Detection Technology Overview

Configuring Deep Discovery Inspector

- Pre-Configuration Console

- Configuring Network Settings
- Configuring System Settings
- Performing Administration Tasks
- Integrating with Syslog Servers
- Deep Discovery Inspector Virtual Analyzer
- Configuring Deep Discovery Inspector Detection Rules
- Avoiding False Positives
- Troubleshooting Deep Discovery Inspector
- 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
- Obtaining Key Information for Analyzing Threat Detections

- Detection Severity Information
- Attack Phase Information
- Detection Type Information
- Suspicious Objects
- Viewing Hosts with Command and Control Callbacks
- Virtual Analyzer Settings

- Virtual Analyzer Cache
- Virtual Analyzer Sample Processing Time
- File Submission Issues

Deep Discovery Analyzer

- Key Features
- Deep Discovery Analyzer Specifications
- Ports Used
- What is Deep Discovery Analyzer Looking For?
- Deep Discovery Analyzer Sandbox
- Scanning Flow
- 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 Key Features
- System Requirements
- 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
- Cyber-Threat Intelligence Sharing
- Threat Sharing Interoperability
- Sharing Advanced Threats and Indicators of Compromise (IOCs) through STIX and TAXII
- Using STIX and TAXII in Deep Discovery Director

Deep Discovery Director - Network Analytics

- Deploying Deep Discovery Director – Network Analytics Overview
- How it Works
- Deploying Deep Discovery Director - Network Analytics
- 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)
- Reviewing Correlation Data Summary
- Viewing the Correlation Data Graph
- Viewing Correlation Data for Suspicious Objects
- Threat Sharing

Preventing Targeted Attacks Through Connected Threat Defense

- Connected Threat Defense Life-Cycle
- Combating Targeted Attacks with Connected Threat Defense
- Key Features of Connected Threat Defense
- Connected Threat Defense Requirements
- Connected Threat Defense Architecture
- Suspicious Object List Management
- Setting Up Connected Threat Defense
- Suspicious Objects Handling Process
- Tracking Suspicious Objects in Deep Discovery Analyzer
- Suspicious Object Sharing Scenarios

Appendices

- What’s new

- Deep Discovery Inspector 5.6
- Deep Discovery Analyzer 6.8
- Deep Discovery Director 5.1 SP1
- Deep Discovery Director - Network Analytics 5.0
- Trend Micro Threat Connect

- Trend Micro Product Integration
- Deep Discovery Threat Detection Technologies
- Creating Sandboxes
- Installing and Configuring Deep Discovery Inspector

Who Should Attend

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
-

Prerequisites & Entry Requirements

General 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

Learning Outcomes

Upon successful completion of this course, participants will be able to:

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
- Configure Deep Discovery Inspector, and enable threat detection
- Setup and use administrative and security management features in:
- Trend Micro Deep Discovery Inspector
- Trend Micro Deep Discovery Analyzer
- Trend Micro Deep Discovery Director
- Trend Micro™ Deep Discovery™ Director – Network Analytics
- 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

Detailed Course Outline

Product Overview

- Trend Micro solutions
- Trend Micro Network Defense

- Key requirements for Trend Micro Network Defense
- Threat classifications
- Trend Micro Network Defense solutions
- Trend Micro Deep Discovery

- Product family

- Deep Discovery capabilities

- Deep Discovery Integration

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 point

- Understanding the attack cycle

- Phases of a targeted attack

- Case study: Pawn storm spear-Phishing

- Deep discovery Threat Detection Technology Overview

Configuring Deep Discovery Inspector

- Pre-Configuration Console

- Configuring Network Settings

- Configuring System Settings

- Performing Administration Tasks

- Integrating with Syslog Servers

- Deep Discovery Inspector Virtual Analyzer

- Configuring Deep Discovery Inspector Detection Rules

- Avoiding False Positives

- Troubleshooting Deep Discovery Inspector

- 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
- Obtaining Key Information for Analyzing Threat Detections

- Detection Severity Information
- Attack Phase Information
- Detection Type Information
- Suspicious Objects
- Viewing Hosts with Command and Control Callbacks
- Virtual Analyzer Settings

- Virtual Analyzer Cache
- Virtual Analyzer Sample Processing Time
- File Submission Issues

Deep Discovery Analyzer

- Key Features
- Deep Discovery Analyzer Specifications
- Ports Used
- What is Deep Discovery Analyzer Looking For?
- Deep Discovery Analyzer Sandbox
- Scanning Flow
- 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 Key Features
- System Requirements
- 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
- Cyber-Threat Intelligence Sharing
- Threat Sharing Interoperability
- Sharing Advanced Threats and Indicators of Compromise (IOCs) through STIX and TAXII
- Using STIX and TAXII in Deep Discovery Director

Deep Discovery Director - Network Analytics

- Deploying Deep Discovery Director – Network Analytics Overview
- How it Works
- Deploying Deep Discovery Director - Network Analytics
- 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)
- Reviewing Correlation Data Summary
- Viewing the Correlation Data Graph
- Viewing Correlation Data for Suspicious Objects
- Threat Sharing

Preventing Targeted Attacks Through Connected Threat Defense

- Connected Threat Defense Life-Cycle
- Combating Targeted Attacks with Connected Threat Defense
- Key Features of Connected Threat Defense
- Connected Threat Defense Requirements
- Connected Threat Defense Architecture
- Suspicious Object List Management
- Setting Up Connected Threat Defense
- Suspicious Objects Handling Process
- Tracking Suspicious Objects in Deep Discovery Analyzer
- Suspicious Object Sharing Scenarios

Appendices

- What’s new

- Deep Discovery Inspector 5.6

- Deep Discovery Analyzer 6.8
- Deep Discovery Director 5.1 SP1
- Deep Discovery Director - Network Analytics 5.0
- Trend Micro Threat Connect
- Trend Micro Product Integration
- Deep Discovery Threat Detection Technologies
- Creating Sandboxes
- Installing and Configuring Deep Discovery Inspector

Skills You Will Learn:

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
- Configure Deep Discovery Inspector, and enable threat detection
- Setup and use administrative and security management features in:
- Trend Micro Deep Discovery Inspector
- Trend Micro Deep Discovery Analyzer
- Trend Micro Deep Discovery Director
- Trend Micro™ Deep Discovery™ Director – Network Analytics
- 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

Frequently Asked Questions

Q: What delivery options are available for Trend Micro Deep Discovery Advanced Threat Detection 3.0 Edition 3 for Certified Professionals?

We offer multiple delivery formats:

- Live Instructor-Led Classroom Online (Virtual/Live Online)
- Traditional Instructor-Led Classroom Training (ILT)
- On-site delivery at your offices anywhere in United Kingdom
- Private dedicated courses customized for your team

Q: What certification does this course prepare me for?

The Trend Micro Deep Discovery Advanced Threat Detection 3.0 Edition 3 for Certified Professionals course helps prepare you for the Certified Professionals Participants explore key concepts and methodologies of using a blend of Deep certification path.

Q: How many CPD hours does this course provide?

The 3-day Trend Micro Deep Discovery Advanced Threat Detection 3.0 Edition 3 for Certified Professionals course provides up to 19.5 CPD hours of structured learning. CPD certificates can be provided upon request.

Q: What is the duration of the Trend Micro Deep Discovery Advanced Threat Detection 3.0 Edition 3 for Certified Professionals training?

The training takes place over 3 day(s), with each day lasting approximately 24.00 hours including breaks for lunch and refreshments.

Q: Do you provide corporate training for Trend Micro Deep Discovery Advanced Threat Detection 3.0 Edition 3 for Certified Professionals?

Yes, we provide corporate training, dedicated training, and closed classes for Trend Micro Deep Discovery Advanced Threat Detection 3.0 Edition 3 for Certified Professionals. Training can take place anywhere in United Kingdom including London, Manchester, Birmingham, Edinburgh, or live online allowing teams from across United Kingdom or internationally to attend.

Q: What related terms do people search for?

Popular related searches include: Trend Micro Deep Discovery Advanced Threat Detection 3.0 Edition 3 for Certified Professionals, Trend Micro, DDATCP

Q: Why choose Nexus Human for Trend Micro Deep Discovery Advanced Threat Detection 3.0 Edition 3 for Certified Professionals?

Nexus Human is recognized as one of the leading training providers. Our trainers have won multiple awards including:

- Small Firms Best Trainer Award
- National Training Partner of the Year (Ireland) - Multiple Years
- Global Top 30 Instructor Awards (2012, 2019, 2021)
- Tech Excellence Award Nominations
- Learning Performance Institute (LPI) External Training Provider Sponsor 2024

Q: Are there any discount codes available?

Yes! Use discount code **PENPAL5** when booking your Trend Micro Deep Discovery Advanced Threat Detection 3.0 Edition 3 for Certified Professionals training. Please note that only one discount code can be used per booking and cannot be combined with other special offers.

Nexus Human

Professional Training & Development

Email: info@nexushuman.com

Website: www.nexushuman.com

Phone: +353 1 XXX XXXX (Ireland) | +44 20 XXXX XXXX (UK)