

## Trend Micro Deep Discovery Advanced Threat Detection 2.1 for Certified Professionals

In diesem Kurs lernen die Teilnehmer, wie man eine Trend Micro™ Deep Discovery Threat Protection-Lösung mit den Komponenten Trend Micro™ Deep Discovery Inspector, -Analyzer und -Email Inspector einsetzt und verwaltet. Dazu erkunden sie die wichtigsten Konzepte und Methoden einer Verknüpfung aus Deep Discovery Lösungen, um eine vollständigere Netzwerksicherheit zu erzielen. Dieser Kurs beschreibt die Grundlagen der Architektur, der Bereitstellungsoptionen, des Threat-Managements und der System-Administration sowie das Troubleshooting und Best Practices für alle drei Produkte. Mit einer Vielzahl von praktischen Übungen wird das erlernte Wissen vertieft. Nach Abschluss des Kurses können die Teilnehmer die Zertifizierungsprüfung zum Trend Micro Certified Professional Deep Discovery ablegen. Die Prüfung ist im Kurspreis inkludiert.

### Kursinhalt

- Übersicht Deep Discovery
- Deep Discovery Features und Benefits
- Installation und Konfiguration von Deep Discovery Inspector, -Analyzer, -Email Inspector und -Director
- Virtual Analyser
- Administration der Lösungen
- Threat Detection Technologien
- Connected Threat Defense

**E-Book** Jeder Teilnehmer erhält ausführliche Kursunterlagen von Trend Micro in englischer Sprache. Wahlweise stellen wir die Printversion oder ein Trend Micro e-Kit zur Verfügung.

### Zielgruppe

Dieser Kurs ist für IT-Profis, die für die IT-Sicherheit und den Schutz von IT-Infrastrukturen verantwortlich sind und sich insbesondere mit komplexen, zielgerichteten Angriffen beschäftigen: System-Administratoren, Network Engineers, Support Engineers, Integration Engineers, Solution & Security Architects.

### Voraussetzungen

Praktische Erfahrungen im Umgang mit den Trend Micro Produkten sowie grundlegende Netzwerkkennnisse werden vorausgesetzt. Außerdem sollten Sie Erfahrung im Umgang mit folgenden Produkten/Technologien haben: Windows Server und Clients, Firewalls, Web Application Firewalls, Packet Inspection Devices, allgemeines Verständnis von Malware.

Für die Registrierung zum Examen wird ein Account im Trend Micro Education Portal benötigt.

### Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: [www.experteach.de/go/TMDD](http://www.experteach.de/go/TMDD)

### Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

### Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

### Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training		Preise zzgl. MwSt.	
<b>Classroom Training</b>	<b>3 Tage</b>	<b>€ 1.895,-</b>	
<b>Termin/Kursort</b>	Kurs Sprache Deutsch		
25.06.-27.06.19 Hamburg	17.12.-19.12.19 Zürich		
23.07.-25.07.19 Zürich	04.02.-06.02.20 Wien		
03.09.-05.09.19 Frankfurt	03.03.-05.03.20 Frankfurt		
21.10.-23.10.19 München	30.03.-01.04.20 München		
19.11.-21.11.19 Hamburg			
<b>Termin/Kursort</b>	Kurs Sprache Englisch		
29.10.-31.10.19 Lausanne			

Stand 21.05.2019



# Inhaltsverzeichnis

## Trend Micro Deep Discovery Advanced Threat Detection 2.1 for Certified Professionals

### Introduction

- Evolving Threats
- Anatomy of a Targeted Attack
- Point of Entry - Spear Phishing
- How Long Can Targeted Attacks Stay Hidden?
- Why Monitor Your Network?
- Why Deep Discovery?

### Deep Discovery Solution Overview

- What is Deep Discovery?
- Deep Discovery Attack Detection
- Deep Discovery Threat Detection Overview
- Deep Discovery Solution Map
  - Trend Micro Deep Discovery Inspector
  - Trend Micro Deep Discovery Analyzer
  - Trend Micro Deep Discovery Email Inspector
  - Control Manager
  - Custom Threat Defense
  - Deep Discovery Director

### Deep Discovery Inspector Overview

- Architecture
- Key Features and Benefits
- Network Setup
- Form Factors
- Deep Discovery Inspector Models
- Deep Discovery Inspector Requirements
- Installation Design
- Positioning Deep Discover Inspector in the Network
- What's new in Deep Discover Inspector 3.8 SP5?

### Deep Discovery Inspector Installation and Configuration

- Information Provisioning for Setup
- Defining Architecture and Traffic to Capture
- Obtaining ISOs, Hot Fixes/Patches
- Performing an Installation
- Configuring Initial System Settings (Pre-Configuration Console)
- Finalizing Deep Discovery Inspector Configuration (Web Console)
- Testing the Deployment
- Viewing Installation Logs
- Enabling IP Rewriting
- Connecting Deep Discovery Inspector to Deep Discovery Director

### Threat Detect Technologies

- Acronyms
- Detection Logic
- Engines versus Detections
- Network Content Inspection Engine (NCIE / VSAPI)
- Advanced Threat Scan Engine (ATSE / VSAPI)
- Network Content Correlation Engine (NCCE / CAV)
- Virtual Analyzer
- Community File Reputation (Census)
- Certified Safe Software Service (CSSS / GRID)
- Trend Micro URL Filtering Engine (TMUFE)
- Network Reputation with Smart Protection Network
- Mobile Application Reputation Service (MARS)
- Summary - Detection Events and Actions

### Virtual Analyzer

- Virtual Analyzer Functionality

### What is Virtual Analyzer Looking For?

- Virtual Analyzer Components
- Communications Flow for Samples
- Overall Sample Ratings and Risk Level
- Virtual Analyzer Outputs
- File Processing Time
- Supported File Types
- How to Explain a Malicious Result
- Sending Files to Virtual Analyzer for Analysis
- Virtual Analyzer Feedback in Deep Discovery Inspector
- Importing a Custom Sandbox into Deep Discovery Inspector for use by the Virtual Analyzer
- Troubleshooting

### Deep Discovery Inspector Administration

- Default Accounts
- Dashboard
- Analyzing Detected Threats
- Running Reports and Obtaining Threat Detection Metrics
- Report Examples
- System Management and Configuration
- Accessing Log Files
- Monitoring System Performance and Resources

### Deep Discovery Analyzer Product Overview

- Key Features
- Network Setup
- Form Factors
- Required Services and Port Information
- Uniquely Identifying Samples
- Integration
- What's New in Deep Discovery Analyzer 5.8?

### Deep Discovery Analyzer Installation and Configuration

- Information Provisioning
- Defining the Architecture
- Obtaining ISOs, Hot Fixes/Patches
- Performing the Installation
- Configuring Initial System Settings
- Configuring Final Settings for Deep Discovery Analyzer
- Testing the Deployment

### Deep Discovery Analyzer Administration

- Accessing the Web Console
- Console Overview
- Analyzing Events
- Submitting Samples to Deep Discovery Analyzer
- Deep Discovery Analyzer Reports
- Managing Suspicious Objects List
- Exceptions
- Deep Discovery Analyzer Sandbox Management
- Reports
- Alerts
- System Management and Configuration

### Deep Discovery Email Inspector

- Key Functionality
- Supported Hardware
- Deployment Modes
- Ports Used

### Summary of Operation Modes

- Threat Detection in Deep Discovery Email Inspector
- Engine Architecture Overview
- What's New in Deep Discovery Email Inspector 2.6?

### Deep Discovery Email Inspector Installation and Configuration

- Information Provisioning
- Defining the Architecture
- Obtain ISOs, Hot Fixes/Patches
- Performing the Installation
- Configuring Initial System Settings using the Pre-Configuration Tool
- Configuring Final Deep Discovery Email Inspector Settings
- Testing the Deployment
- Connecting Deep Discovery Email Inspector to Deep Discovery Director

### Deep Discovery Email Inspector Administration

- Management Console Overview
- Analyzing Threat Detections
- Configuring Policies
- Setting up Recipient Notifications
- Defining Email Message Tags
- Configuring Redirects (Non-Scannable Attachments)
- Adding Policy Exceptions
- Configuring Alerts
- Generating Reports
- Accessing Log Files
- System Administration
- Performing System Maintenance Tasks

### Threat Connect

- Content
- Using Threat Connect
- Report Content

### Connected Threat Defense

- Integration is Key to Effective Security
- Connected Threat Defense Requirements
- Connected Threat Defense Components
- Integrating Deep Discovery Inspector with Control Manager
- Suspicious Objects Handling with Control Manager

### Integration

- Open Architecture
- Deep Discovery Inspector Integration
- Integration with Syslog Servers and SIEM Systems
- Third-Party Blocking Integration
  - Check Point Open Platform for Security
  - HP TippingPoint Security Management System
  - IBM Security Network Protection
  - Palo Alto Firewalls
  - Blue Coat ProxySG
- Deep Discovery Analyzer Integration

### Appendix 1: Monitoring VM Traffic with Deep Discovery Inspector

- Overview
- vDS Remote Monitoring Feature
- Implementation
- Configuration



### ExperTech GmbH

Waldstraße 94 • 63128 Dietzenbach • Telefon: +49 6074 4868-0 • Fax: +49 6074 4868-109  
info@expertech.de • www.expertech.de

