

Trend Micro Deep Discovery Advanced Threat Detection Training 4.0 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, -Director und Director – Network Analytics einsetzt und verwaltet. Dazu erkunden sie die wichtigsten Konzepte und Methoden einer Verknüpfung aus Deep Discovery Lösungen, um eine vollständigere Netzwerksicherheit zu erzielen.

Es wird ein umfassender Überblick über den Zweck, die Funktionen und Fähigkeiten von Deep-Discovery-Netzwerksicherheitslösungen gegeben, einschließlich Empfehlungen zu bewährten Verfahren und allgemeinen Schritten zur Fehlerbehebung für eine erfolgreiche Implementierung und langfristige Wartung einer Deep-Discovery-Umgebung.

Der Kurs befasst sich auch mit verschiedenen Einsatzüberlegungen und -anforderungen, die erforderlich sind, um Deep Discovery-Lösungen in verschiedene andere Trend Micro Produkte einzubinden, um einen synchronisierten Austausch von Bedrohungsinformationen für eine erweiterte Bedrohungserkennung zu ermöglichen.

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

- Product Overview
- Deep Discovery Inspector
- Configuring Deep Discovery Inspector
- Analyzing Detected Threats in Deep Discovery Inspector
- Deep Discovery Analyzer
- Deep Discovery Director
- Deep Discovery Director – Network Analytics
- Preventing Targeted Attacks Through Connected Threat Defense

E-Book Sie erhalten 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.ch/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.	
Termine in Deutschland		3 Tage CHF 2.195,-	
Online Training		3 Tage CHF 2.195,-	
Termin/Kursort		Kurs Sprache Deutsch 	
21.05.-23.05.24	 München	19.08.-21.08.24	 Online
21.05.-23.05.24	 Online	25.11.-27.11.24	 München
19.08.-21.08.24	 München	25.11.-27.11.24	 Online

Stand 24.02.2024



Inhaltsverzeichnis

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

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

