Enterprise Computing Solutions - Education Services

TRAINING OFFERING

Puoi raggiungerci qui

Arrow ECS Srl - Via Lancia 6/a - 39100 Bolzano

Email: training.ecs.it@arrow.com
Phone: +39 0471 099 134

Trend Micro Deep Discovery for Certified Professionals

CODE:	LENGTH:	PRICE:
TRM_DD-CP	24 Hours (3 days)	€1,500.00

Description

In this course, you will learn how to use Trend Micro™ Deep Discovery This course provides information about the basic architecture, deployment scenarios, installation, configuration, and administration options, and troubleshooting details that an administrator needs to know for successful implementation and long-term maintenance.

Objectives

In this course, you will learn how to use Trend Micro™ Deep Discovery

Audience

This course is designed for IT professionals who are responsible for protecting networks from any kind of networked, endpoint, or cloud security threats. The individuals who will typically benefit the most include:

- System administrators
- Network engineers
- Support Engineers
- Integration Engineers
- Solution & Security Architects

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. You should also have a working knowledge of the following products:

- 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 screen resolution of at least 1980 x 1080 or above; a display size of 15" or above is recommended.

Programme

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
  - o Trend Micro Deep Discovery Inspector
  - o Trend Micro Deep Discovery Analyser
  - o Trend Micro Deep Discovery Email Inspector
  - o Control Manager
  - o Custom Threat Defence
  - o 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 Analyser
- 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
  - o Check Point Open Platform for Security
  - o HP TippingPoint Security Management System
  - o IBM Security Network Protection
  - o Palo Alto Firewalls
- Blue Coat ProxySG
- Deep

Follow on courses

Please contact us training.ecs.it@arrow.com

Test and Certification

This course is taught by Trend-Micro certified trainers. Upon completion of this course, participants may complete the certification examination to obtain designation as Trend Micro Certified Professional for Deep Discovery.

Further Information

For any other information please contact training.ecs.it@arrow.com putting your contacts. You will be called back ASAP

Session Dates

Su richiesta. Contattaci al n.ro +39 0471 099134 oppure via mail a training.ecs.it@arrow.com

Informazioni aggiuntive

Questa formazione è disponibile anche come formazione in loco. Per favore, contattaci per saperne di più.