Trellix

DATASHEET

ATD with DXL, TIE and MAR Administration

Education Services Instructor-led Training

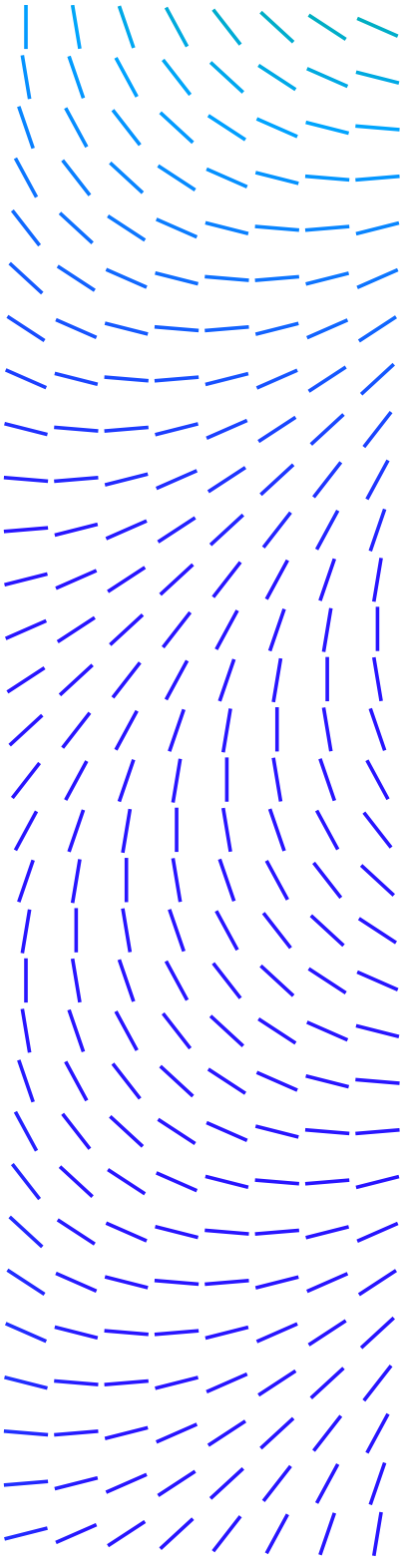
Introduction

Our ATD with DXL, TIE and MAR Administration course provides an in-depth look at each of the products and how they integrate with each other. In this course, you will learn the tasks crucial to set up, administer, and manage Advanced Threat Defense (ATD), Data Exchange Layer (DXL), Threat Intelligence Exchange (TIE), and Active Response (MAR) solutions. This combined solution enables you to gain better visibility to your environment, protecting and limiting exposure to threats and vulnerabilities. This course combines lectures and practical lab exercises with significant time allocated for hands-on interaction with the ATD, TIE, DXL, and MAR user interfaces, as well as detailed instructions for the integration of this solution.

> In this course, you will learn the tasks crucial to set up, administer, and manage Advanced Threat Defence (ATD), Data Exchange Layer (DXL), Threat Intelligence Exchange (TIE), and Active Response (MAR) solutions.

Audience

This course is intended for system and network administrators, security personnel, auditors, and/or consultants concerned with system endpoint security.



Agenda At A Glance

Day 1:

- Welcome
- Products Integration
- Advanced Threat Defense Solution Overview
- ATD Installation and Set up
- Configuring ATD Appliance Settings
- Creating Virtual Machines in ATD

Day 2:

- Malware Analysis in ATD
- Configuring ATD Cluster
- Managing Content and Basic Troubleshooting in ATD
- Data Exchange Layer Overview
- Threat Intelligence Exchange Overview
- Active Response Overview

Day 3:

- DXL, TIE, and MAR Installation
- Managing, Configuring, and Troubleshooting DXL
- Configuring and Using TIE
- Configuring and Using MAR

Day 4:

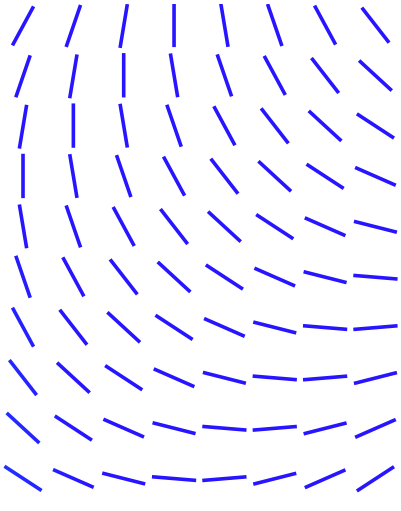
- Using MAR Threat Workspace, Health Status, and Remediation History
- ATD Integration with ePO, DXL, TIE, and MAR
- ATD Integration with MWG and NSP
- ATD Integration with Email Connector and ESM

Recommended Pre-Work

- Basic knowledge of network concepts and protocols (TCP/IP)
- Basic understanding of routing and connecting flow (LAN, WAN, Internet)
- Basic knowledge of Operating Systems (Windows and Linux)
- Working knowledge of ePolicy Orchestrator (ePO)

Related Courses

- Advanced Threat Defense Administration
- Endpoint Security Administration
- DXL 6.0 Essentials
- TIE 2.0 Essentials
- Active Response 2.2 Essentials



Course Learning Objectives

- Describe ATD solution purpose, key features, and benefits.
- Install and configure ATD appliance settings.
- Create VM and analyzer profiles in ATD to be used for analysis.
- Submit content to ATD for analysis, interpret the results, generate reports, and manage the whitelist and blacklist.
- Update security content and software in ATD.
- Identify resources and tools useful for basic troubleshooting in ATD.
- Describe the DXL, TIE, and MAR solutions, requirements, and key features.
- Install and verify TIE, DXL, and MAR components.
- Configure basic policies for DXL brokers and clients.
- Configure the DXL broker in ePO.
- Describe and perform basic troubleshooting tasks for DXL.
- Identify and configure policies required for a TIE environment.
- Analyze and manage threat reputation.
- Explain how to configure the Active Response service from ePO.
- Explain how to use MAR collectors, searches, reactions, and triggers.
- Use Threat Workspace to investigate malware.
- Integrate ATD with selected McAfee solutions and explain how to operationalize the solutions to deliver specific outcomes.