DATASHEET

Trellix Intelligent Sandbox with DXL and TIE Administration

Education Services Instructor-led Training

Introduction

Our Trellix Intelligent Sandbox with DXL and TIE Administration course provides an in-depth look at each of the products and how they integrate. In this course, you will learn the tasks crucial to set up, administering, and managing Trellix Intelligent Sandbox (TIS), Data Exchange Layer (DXL), and Threat Intelligence Exchange (TIE) solutions. This combined solution enables you to gain better visibility of 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 TIS, DXL, and TIE user interfaces, as well as detailed instructions for the integration of this solution.

Audience

This course is intended for system and network administrators, security personnel, auditors, and/or consultants concerned with network and system security. It is recommended that the students have a basic knowledge of network concepts and protocols (TCP/IP), a basic understanding of routing and connecting flow (LAN, WAN, Internet), basic knowledge of Operating Systems (Windows/Linux), and a working knowledge of ePolicy Orchestrator.

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

- ePolicy Orchestrator Administration
- Endpoint Security Administration
- DXL Essentials
- TIE Essentials

Agenda at a Glance

Day 1:

- Welcome
- Products Integration
- Trellix Intelligent Sandbox Solution Overview
- TIS Installation and Setup
- Configuring TIS Appliance Settings
- Creating Virtual Machines in TIS

Day 2:

- Malware Analysis in TIS
- Configuring TIS Cluster
- Managing Content and Basic Troubleshooting in TIS
- Data Exchange Layer Overview
- Threat Intelligence Exchange Overview
- What is Endpoint Detection and Response?

Day 3:

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

Day 4:

- TIS Integration with ePO, DXL, TIE, AR, and EDR
- TIS Integration with SWG and NSP
- TIS Integration with Email Connector and ESM

Learning Objectives

Welcome

Become familiar with ePO information and support resources and feedback mechanisms.

Products Integration

Describe the integration framework, how to integrate products with TIS, and the use case for dealing with threats.

Trellix Intelligent Sandbox Solution Overview

Describe the TIS solution, its features, and its functionality.

Installation and Setup

Describe how to install the TIS appliance and configure the initial settings.

Configure Appliance Settings

Describe how to configure settings on the TIS appliance.

Creating Virtual Machines

Describe how to create Virtual Machines (VMs) and Analyzer Profiles on TIS.

Malware Analysis

Describe how to perform malware analysis, view analysis status, analyze reports, and generate reports on TIS.

Configuring a TIS Cluster

Describe a TIS cluster, configure, and destroy TIS clustering and network connections.

Managing Content and Basic Troubleshooting

Describe how to manage content and basic troubleshooting in TIS.

Data Exchange Layer Overview

Describe the DXL solution, its features, and its functionalities.

Threat Intelligence Exchange Overview

Describe the TIE solution, its features, and its functionalities.

Endpoint Detection and Response Overview

Describe the EDR solution, its features, and its functionalities.

DXL and TIE Installation

Describe how to install DXL and TIE Extensions and check-in packages on ePO. Describe how to install the TIE server and DXL broker.

Managing, Configuring, and Troubleshooting DXL

Describe how to configure policies for DXL brokers and clients, configure DXL broker in ePO, functionalities of DXL fabrics, and perform basic troubleshooting tasks in DXL.

Configuring and Using Threat Intelligence Exchange

Describe how to configure the TIE server for VirusTotal, configure policies and use server tasks for ongoing maintenance and perform basic TIE troubleshooting tasks.

TIS Integration with ePO, DXL, TIE, AR, and EDR

Describe how to integrate TIS with SWG and IPS solutions.

TIS Integration with SWG and IPS

Describe how to integrate TIS with SWG and IPS solutions.

Ordering or Information

To order, or for further information, please email SecurityEducation@trellix.com

About Trellix

Trellix is a global company redefining the future of cybersecurity and soulful work. The company's open and native extended detection and response (XDR) platform helps organizations confronted by today's most advanced threats gain confidence in the protection and resilience of their operations. Trellix, along with an extensive partner ecosystem, accelerates technology innovation through machine learning and automation to empower over 40,000 business and government customers with living security. More at https://trellix.com.