TRELLIX

Threat Intelligence Exchange with Intelligent Virtual Execution - Server Administration
Instructor-Led Training

Highlights

Duration

4 days

Prerequisites

Students taking this course should have a solid knowledge of Windows and system administration and network technologies, as well as a basic understanding of computer security and concepts.

How to Register

This course is available for purchase at https://training-catalog.trellix.com/.

Private sessions are available. For further details and pricing, please contact your Trellix account representative.

Instructor-led sessions are typically a blend of lecture and hands-on lab activities. To view our full course catalog, please visit https://training-catalog.trellix.com/.

This course provides an in-depth look at each of these Trellix products and how they integrate. In this course, you will learn the tasks crucial to configure, administer, manage, and troubleshoot Intelligent Virtual Execution (IVX), 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 IVX, DXL, and TIE user interfaces, as well as detailed instructions for the integration of this solution.

Learning Objectives

After completing this course, learners should be able to:

- Describe the DXL and TIE solutions, requirements, and key benefits and how they integrate with IVX - Server

- Install and verify TIE and DXL

- Configure and manage TIE and DXL

- Set up the environment and deploy IVX - Server

- Administer and manage an IVX - Server solution

- Perform malware analysis using IVX - Server

- Describe the IVX - Cloud product and how it works

- Discuss IVX integration with other Trellix products and resulting benefits

- Migrate IS to IVX - Server

- Identify resources and tools useful for basic troubleshooting in TIE, DXL, and IVX - Server

Who Should Attend

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

Course Outline

Day 1

1. Welcome
2. Products Integration (IVX/TIE/DXL)
3. DXL Overview
4. TIE Overview
5. DXL and TIE Installation
6. DXL and TIE Upgrade

Day 2

7. DXL Configuration and Management
8. TIE Configuration and Integration with IVX
9. TIE Reputations
10. TIE Server Maintenance

Day 3

11. IVX Solution Overview
12. IVX Deployment
13. Central Management Integration & Cluster Configuration

14. IVX Configuration
15. IVX Analysis
16. IVX Integration with HX, NX, EX, and FX
17. IVX - Cloud

Day 4

18. IS Migration to IVX
19. IVX Integrations Advanced Malware Detection with IVX/IPS Integration
20. Troubleshooting
21. Dashboards, Queries, and Reports

Appendices:

22. YARA Rules
23. SIEM Integration Labs

022024-15