Trellix

EDUCATION SERVICES

Network Detection and Response (NDR) Administration

Instructor-Led Training

Highlights

Duration

1 day

Prerequisites

A working understanding of the command line interface (CLI) and the Linux Operating system, and familiarity with network security.

How to Register

Public sessions are listed at https://trellix-training.netexam.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://trellix-training.netexam.com.

Introduction

This one-day hands-on course focuses on configuring and administering NDR systems, specifically Network Investigator and Packet Capture. Participants will engage in practical labs to integrate existing Trellix sensors, such as Network Security and Intrusion Prevention System, into the NDR environment. The course provides an overview of each appliance, their standard network deployments, and how they function within the NDR system alongside the sensors.

Lab exercises are included in this course.

Learning Objectives

After completing this course, learners should be able to:

- Provide an overview of the NDR sensors that integrate with the Trellix NDR-enabled Network Investigator system.
- Integrate NDR sensors including Network Security and Intrusion Prevention System with Network Investigator for export of metadata, flow, and alerts.
- Configure and integrate Trellix Packet Capture with Network Investigator for packet capture retrieval.
- Enable NDR machine learning (ML) detection modules.
- Describe other NDR features and integrations including Asset Discovery and Trellix Logon Collector.
- Illustrate the typical deployment of Packet Capture and Network Investigator in the context of other Trellix systems.
- Access the various administration interfaces for Packet Capture and Network Investigator.
- Perform primary management and administration tasks for Packet Capture and Network Investigator.

Who Should Attend

Network security professionals who administer and operate Trellix Network Investigator and Packet Capture and integrate Intrusion Prevention System, and Network Security as NDR sensors along with other Trellix technologies.

Course Outline

1. **Introduction to NDR**
   - NDR Overview
   - Packet Capture (PX)
   - Packet Capture Deployments
   - Network Forensics Basic Hardware Components
   - Traffic Retention and Disk Usage Considerations
   - Network Security (NX)
   - Network Security Deployment with Packet Capture
   - Intrusion Prevention System (IPS)
   - IPS Sensor Deployment with Packet Capture
   - Network Investigator (NI)
   - Network Investigator Deployments
   - NDR Modules
   - NDR Deployments: NI-PX-NX and NI-PX-IPS
   - Other Network Investigator Integrations
2. **Network Forensics Configuration**
   - NI and PX Admin Interfaces
   - The CLI
   - Accessing Admin-Level Commands
   - Configuration Mode
   - Accessing the Web
   - Post-Install Configuration
   - Dynamic Treat Intelligence (DTI) Cloud
   - Configure Network Time Protocol (NTP) Server
   - Configure Capture
   - Verify Data on Packet Capture (PX)
   - Lab: Configure Packet Capture and Network Investigator
3. **Network Forensics Administration**
   - Authentication
   - Creating Local Users
   - Assigning Roles
   - Managing the System
   - Processes
   - Logs
   - System Health Tools
   - Show Command
   - Network Investigator Appliance Groups
   - Software Updates
   - Configuring Event Based Capture (EBC)
   - Packet Capture Metadata Filtering
   - DNS Aggregation
4. **Configuring NDR Integrations**
   - NDR Sensor Integrations
   - Pair a Packet Capture (PX) with Network Investigator (NI)
   - NDR Deployments: NI-PX-NX
   - NDR Deployments: NI-PX-IPS
   - Verifying NDR Integrations
   - Other NDR Integrations
   - Trellix Logon Collector (TLC)-NI
   - Critical Asset Discovery (CAD)
   - Lab: Pair Packet Capture and Network Investigator
   - Lab: Configure NDR Integrations

Visit Trellix.com to learn more.

052024-06