NT-TETADV: Tetration Firewall Enforcement Agents, Data Flow Mapping, and Advanced Policy Deployment

Course Code: NT-TETADV
Duration: 5 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

Tetration Firewall Enforcement Agents, Data Flow Mapping, and Advanced Policy Deployment is a 5-day course exploring telemetry data, the flows corpus, and how Cisco Tetration Analytics™ Firewall Agent provides enforcement.

This course will provide the details and hands-on activities necessary to successfully deploy, manage, and troubleshoot firewall policies in Cisco Tetration.

SKILLS COVERED

Upon completing this course, the learner will be able to understand how Cisco Tetration AnalyticsTM:

- Describe how the Cisco Tetration Firewall Agent works to enforce security policy
- Describe how to deploy the Cisco Tetration Firewall Agent
- Describe how to Manage and Troubleshoot Cisco Tetration Firewall Agent policies
- Review administrative and management tasks necessary to operate, support and manage Tetration
- Describe how Tetration telemetry data is utilized in the Flows Corpus
- Construct effective policies based on discovered flows and Application Dependency Mapping (ADM)

WHO SHOULD ATTEND?

The primary audience for this course is as follows:

- System Engineers
- Network Engineers
- Technical Managers
- System Administrators
- System Architects
- Technical Decision Makers

PREREQUISITES

The knowledge and skills that the learner should have before attending this course are as follows:

- Knowledge of cloud and (virtual) data center architecture or cloud basic networking concepts
- Familiarity with Cisco basic networking security concepts and application security concepts
- High-level familiarity with basic telemetry protocols and Big Data analytics

MODULES

Module 1: Cisco Tetration Firewall Agent

- How the Cisco Tetration Firewall Agent Enforces Firewall Rules
- Deploying and Managing Linux Enforcement Agents
- Deploying and Managing Windows Enforcement Agents
- Deploying and Managing AIX Enforcement Agents

Module 2: Tetration Enforcement Agent Components, Messaging, and Interaction

- Enforcement Front End
- Firewall and Catch-all Rules

- The Preserve Rules Option
- Agent Config Intents
- Stateful Enforcement

Module 3: Tetration Enforcement Agent UI Configurations and Troubleshooting

- Agent UI Configuration
- Monitoring Agents
- Platform Specific Enforcement Features and Requirements
- Known Limitations
- Troubleshooting Inbound and Outbound Firewall Rules

Module 4: Tetration Secure Connector, Edge and Ingest Appliances

- Tetration Secure Connector Overview
- Tetration Secure Connector features and configuration
- Tetration Edge Appliance Overview
- Tetration Edge Appliance configuration
- Tetration Ingest Appliance Overview
- Tetration Ingest appliance features and configurations

Module 5: Application Dependency Mapping

- Application Management Workflow Cycle
- Tetration Application Insight
- ADM Process
- ADM Run Results
- Cluster Confidence

Module 6: Tetration Policy Analysis

- Enable Policy Analysis
- Live Policy Analysis
- Backdated Policy Experiments
- Quick Policy Analysis
- Diagnosis Using Policy Analysis

Module 7: Cisco Tetration Analytics Policy Enforcement Overview

- Policy Global Ordering & Conflict Resolution
- Scope Priorities
- Troubleshooting Policy Enforcement

Module 8: Cisco Tetration Flow Search

- Understanding the Flow Corpus
- Using Scopes to Filter Results
- Searching with Conjunctions
- Correlating Flow Data with Hosts and Processes
- Leveraging Annotations

Module 9: Using Tetration Forensics

- Forensic Signals
- Configuring Forensics
- Forensics Visualization and Alerts
- Forensics Scoring
- Network and Process Hash Anomaly Detection

Module 10: Tetration Apps and API

- App Store
- User Apps
- Visualize Data Sources
- Bring your own Data
- OpenAPI

END OF PAGE