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

Course 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
- ForensicsScoring
- Network and Process Hash Anomaly Detection

- Module 10: Tetration Apps and API
  - App Store
  - User Apps
  - Visualize Data Sources
  - Bring your own Data
  - OpenAPI

Labs:

Labs are designed to assure learners a whole practical experience, through the following practical activities:

- Cisco Tetration GUI Familiarization
  - Task 1: Log in to the Tetration Cluster and Explore the Security Dashboard
  - Task 2: Explore the Visibility Dashboard
  - Task 3: Explore the Visibility Flow Search Options
  - Task 4: Explore the Visibility Inventory Search Options

- Software Agent Installation
  - Task 1: Configure Agent Intents
  - Task 2: Install the Tetration Enforcement Agent for Linux
  - Task 3: Install the Tetration Enforcement Agent for Windows
  - Task 4: Monitor Enforcement Agent Status

- Importing Context Data
  - Task 1: Upload User-Defined Annotations
  - Task 2: View User-Defined Annotations

    - Task 3: Search by User-Defined Annotations

- Scopes
    - Task 1: Navigate Scopes
    - Task 2: Create a Scope
    - Task 3: Edit a Scope

- Application Dependency Mapping with Agents
    - Task 1: Create an Application Workspace
    - Task 2: Examine Conversations
    - Task 3: Examine Endpoint Clusters
    - Task 4: Create an Application View

- Implementing Policy
    - Task 1: Gather IP Address Information
    - Task 2: Create the Server Load Balancing Information File
    - Task 3: Create an Application Workspace
    - Task 4: Review Day 0 and Automated Policies

- Policy Enforcement and Compliance
    - Task 1: Enable Policy Enforcement and Compliance
    - Task 2: Test Policy Enforcement and Compliance
    - Task 3: Monitor and Troubleshoot Policy Enforcement Status and Compliance

- Workload Security
    - Task 1: Review Packages and CVE Reports
    - Task 2: Review Policy Enforcement
    - Task 3: Review Rule Order and Efficiency

- Secure Connector, Edge and Ingest Appliances
    - Task 1: Review Tetration Secure Connector deployment and configurations
    - Task 2: Review Tetration Edge and Ingest Appliance deployment and configurations